Statement of Inspector General Kathleen S. Tighe

U.S. Department of Education

Before the Committee on Oversight and Government Reform and the

United States House of Representatives

November 17, 2015

Chairman Chaffetz, Ranking Member Cummings, and the members of the Committee on Oversight and Government Reform:

Thank you for inviting me here today to discuss the work of the U.S. Department of Education (Department) Office of Inspector General (OIG) involving information technology security at the Department. The explosion of information technology (IT) has revolutionized the way the world does business—and the Department is no exception. Virtually every Department program relies heavily on information systems. Evaluating whether those information systems are secure and operating effectively is a top priority for the OIG.

The Federal Information Security Management Act of 2002, as amended by the Federal Information Security Modernization Act of 2014 (FISMA), requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the data and data systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. It also requires inspectors general to annually evaluate agency information security programs and practices. I will focus my testimony on the results of our fiscal year (FY) 2015 FISMA audit, as well as other recent work that my office has conducted related to information security.

Background on the Department's IT Systems and System Security Responsibilities

The Department reports184 information systems in its inventory, more than 120 of which are operated by contractors or subcontractors, some of which contain sensitive financial information and personally identifiable information (PII) pertaining to millions of student aid applicants and recipients, grantees, and others. The following are the key areas and systems that we focused our work on this year:

- The Education Department Utility for Communications, Applications, and Technology Environment (EDUCATE) contract established a contractor-owned, contractor operated service model for the Department. Under this contract, Dell Services Federal Government (Dell) provides the network infrastructure and an enterprise-wide IT environment, which includes services such as email, network servers, desktop support, security, and printers.

- The Department's office of Federal Student Aid (FSA) also has a large Virtual Data Center (VDC), currently run by Dell, which serves as the hosting environment for FSA business systems such as 1) the National Student Loan Data System (NSLDS), the central database for Federal student aid, which stores information about loans, grants, borrowers, lenders, schools, services, and guaranty agencies (GAs), and 2) the Central Processing System (CPS), which processes all applications for Federal student aid, calculates financial aid eligibility, and notifies students and educational institutions of the results of the eligibility calculation. Both NSLDS and CPS contain sensitive financial information and PII.

- FSA also relies on the Common Origination Disbursement (COD) system, through which funds to eligible students and schools for the Federal student aid programs are delivered and tracked. COD resides in two data centers: one in Plano, Texas, currently managed by Dell at the VDC, and the second in Columbus, Georgia, managed by Total Systems Services, Inc. (TSYS), under the Department's prime contract with Accenture. Like NSLDS and CPS, the COD system also contains sensitive financial information and PII.

In recent years, the Department has experienced sophisticated attacks on its IT systems, including from hostile websites accessed by employees and phishing campaigns resulting in malware infections, as well credentials stolen from employees or external business partners through keystroke loggers.

Results of Recent OIG Reviews and Investigations

The Department's and FSA's information security controls are examined every year through the OIG's FISMA audit and in the annual financial statement audits of the Department's and FSA's financial statements. We also have conducted other IT-related work outside of our FISMA and financial statement work. All of our work has identified oversight and system deficiencies that impact the security and jeopardize the reliability of information within the Department and contractor systems.

In 2013, I testified before this Committee on recommendations made in OIG reports that the Department had not yet implemented. One area I highlighted was our finding the same deficiencies over and over again, known as repeat findings, particularly in our information security audits. Since my 2013 testimony, repeat findings continue to be an issue in the area of information security. For example:

- In our FY 2014 FISMA audit, we identified findings in 6 of the 11 security control areas reviewed—configuration management, identity and access management, incident response and reporting, risk management, remote access management, and contingency planning. In addition, in 5 of these 6 areas we had repeat findings from reports issued during the prior 3 years. We also found, in some instances, that although the Department said it had completed its actions to address a recommendation, we continued to find that corrective actions were not implemented. Our FY 2015 FISMA audit identified 6 repeat findings in 4 of 10 areas. I will discuss the results of our FY 2015 FISMA audit in more detail below.

- Likewise, since 2009, including this year, audits of the Department's and the FSA's financial statements, conducted by an independent auditor that the OIG oversees, have found persistent IT control deficiencies in key financial systems. The independent auditor has found that the Department and FSA need to mitigate persistent control deficiencies in the areas of security management, personnel security, access controls, and configuration management across those systems. Failure to correct the deficiencies can increase the risk of unauthorized access to the Department's systems and could affect the reliability and security of the data and information stored in those systems.

The OIG has issued other reports over the last several years that identified issues with the Department's and FSA's oversight and monitoring of information security controls of program participants. For example:

- Our 2014 review of FSA's oversight and monitoring of private collection agencies' (PCA) and GA's information security documents found that FSA did not adequately process PCA system reauthorizations such that PCA's operated without valid authorizations for an average of 8 months, did not ensure that PCAs timely resolved security control deficiencies, and had inadequate assurance that GA information system security complied with the FISMA requirements. PCAs and GAs process Department student loan account records on their own computer systems and connect with various Department systems containing student loan information. FSA has recently taken some steps toward enhancing the security posture of the GAs.

- Our 2013 examination of FSA's Personal Identification Number (PIN) registration system, which provided students and their parents access to their personal records on FSA Web sites, such as fafsa.ed.gov and pin.ed.gov, identified security vulnerabilities that had allowed unauthorized users to access the PIN system. After our review, FSA replaced the PIN system with the more secure Person Authentication Service (PAS) system in May 2015.

FY 2015 FISMA Results

The FISMA evaluations for the OIGs had two new features this year. First, the FISMA Modernization Act of 2014 requires the OIGs this year for the first time to evaluate the effectiveness of their agency's security program and practices. As set forth in National Institute of Standards and Technology (NIST) guidance, "effectiveness" addresses the extent to which security controls are implemented correctly, operate as intended, and produce the desired outcome. Second, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), in coordination with the Office of Management and Budget (OMB), the U.S. Department of Homeland Security, and others, rolled out the first phase of its new FISMA evaluation metrics—the maturity model. The model has as its foundation the NIST effectiveness standard but uses attributes that provide perspective on the overall status of information security within an agency, as well across agencies. It summarizes the status of information security programs and their maturity on a 5-level scale (with 5 being the best). The first phase encompasses the FISMA security area of continuous monitoring management; CIGIE plans to extend the model to other FISMA security areas in 2016.

Our FY 2015 FISMA audit found that the Department was at level 1 for continuous monitoring management, and was not generally effective in three additional areas—configuration management, incident response and reporting, and remote access management. Specifically we found:

- Continuous Monitoring Management: The Department's overall continuous monitoring program only met attributes for level 1 of the CIGIE maturity model, and thus was not effective. Level 1 means that its continuous monitoring program is ad-hoc—not formalized and activities are performed in a reactive manner. Although the Department defined how it will implement its continuous monitoring activities, related processes, performance measures, policies, and procedures have not been implemented consistently across the Department. However, under OMB requirements, agencies have until FY 2017 to fully implement continuous monitoring of security controls. The Department has developed a project plan to address the timely implementation of a continuous monitoring program that meets NIST requirements. The goal of continuous monitoring is to maintain ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Until continuous monitoring is fully implemented, the Department will continue to rely upon manual processes.

- Configuration Management: The Department's configuration management program was not generally effective because of key weaknesses in application connection protocols; unsupported operating systems in the production environment; interface connections operating on expired certificates; inability to detect unauthorized devices connecting to the network; and weaknesses in identifying and resolving configuration management vulnerabilities in the EDUCATE environment. These weaknesses are concerning because they create vulnerabilities that could potentially allow unauthorized users to gain access to Department systems and resources. We also found that although some of the Department's information security policies for configuration management were outdated, they were consistent with NIST requirements; and that the Department has processes for maintaining and updating inventories for systems, connections, operating systems, and web certificates.

- Incident Response and Reporting: The Department's overall incident response and reporting program is not generally effective because we identified key weaknesses in its internal intrusion detection and prevention of system penetrations. Specifically, during our testing of the EDUCATE environment, OIG testers were able to gain full access to the Department's network and our access went undetected by Dell and the Department's Office of the Chief Information Officer. However, we found the Department was generally effective at ensuring proper incident response and reporting once incidents are reported because it had policies and procedures consistent with NIST requirements; it had established a real-time security operations center; and it had a process that operated to track, monitor, and resolve security incidents. An organization's incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited to prevent future occurrences, and restoring IT services.

- Remote Access Management: The Department's remote access management program was not generally effective mainly because it did not have a complete remote access inventory and did not use two-factor authentication for two of its external network connections. Further, after we notified the Department of this vulnerability, it took approximately 6 months for them to apply two-factor authentication to these two connections. We found that the severity and impact of not enforcing two-factor

> authentication on these particular network connections could result in a potential compromise of Department resources.

We determined that three areas—risk management, security training, and contingency planning—were generally effective, although some improvements were needed. For the Department's plan of action and milestones process, we determined that if the established policies and practices are implemented as intended, it should be effective. We also determined that the Department's identity and access management programs and practices would be generally effective if implemented properly, but that the Department's controls over access to FSA's mainframe environment need improvement.

We did not make a separate conclusion on the effectiveness of the Department's program to oversee the security of contractor systems because, given that the Department relies almost exclusively on contractors to operate its systems, our assessment of information security management included in our FISMA report addressed issues of contractor oversight. However, our review specifically found that FSA did not have reasonable assurance that commercial users of a mainframe environment supporting the COD system operated by the subcontractor TSYS do not have access to Department data. During our FISMA audit, TSYS refused to provide the OIG with documentation reflecting a complete listing of all userids with privileges on the mainframe. After repeated requests, TSYS provided a copy of Education userids with privileges, but redacted all other userids with privileges in the mainframe environment. Without this data, the OIG was unable to complete a comprehensive vulnerability assessment of the environment and determine whether other customers on the mainframe could improperly access Department data.

This is particularly problematic because based on the information TSYS did provide regarding the mainframe users, we found accounts with excessive permissions and unauthorized access.

To address the issues identified in our FISMA audit, we made 26 recommendations—16 new recommendations and 10 repeat recommendations, including that the Department direct Accenture to obtain a complete list of userids from TSYS and produce it to FSA and the OIG; and, in the event of refusal or inability to produce the requested information, take appropriate action under the contract or other authority to ensure that Department data hosted by TSYS on the COD mainframe is adequately safeguarded from unauthorized access.

Closing Statement

In light of recent high-profile data breaches at other Federal agencies, the importance of safeguarding the Department's information and information systems cannot be understated. The Department's systems house millions of sensitive records on students, their parents, and others, and facilitate the processing of billions of dollars in education funding. These systems are primarily operated and maintained by contractors and are accessed by thousands of authorized individuals (including Department employees, contractor employees, and other third parties such as school financial aid administrators). Protecting this complex IT infrastructure from constantly changing cyber-threats is an enormous responsibility and challenge. While the Department and FSA have both made progress and taken steps to address past problems that we have identified, our work this year demonstrates once again that they remain vulnerable to attacks and that there are key areas where immediate action and attention are needed. As noted, our penetration testing this year revealed a key weakness regarding the Department's ability to detect unauthorized activity inside its computer networks that needs to be addressed promptly. Likewise, our work looking at access to data processed on FSA mainframes raises significant concerns over the Department's and FSA's ability to adequately oversee its contractors and ensure that only individuals with appropriate permissions have access to Department data. Our recently issued report highlights numerous areas that need to be improved in order to develop a better IT security program. My office is committed to helping Department and FSA officials strengthen information security controls and mitigate risks to their systems and the valuable data they hold. The Department and FSA must work harder to address existing weaknesses so they can be in a better position to identify and stop ever-evolving cyber threats and increasingly sophisticated attacks on critical IT infrastructures. That concludes my written statement. I am happy to answer your questions.