Written Testimony
Jason K. Gray
Chief Information Officer
U.S. Department of Education

"Examining the Cybersecurity Incident that Affected the IRS Data Retrieval Tool"
Before the U.S. House of Representatives Committee on Oversight and Government Reform

May 3, 2017

Good morning Mr. Chairman, Ranking Member Cummings, and Members of the Committee. I am Jason Gray, Chief Information Officer (CIO) for the U.S. Department of Education ("Department"), a position I have had the privilege of holding since June, 2016.

I appreciate the opportunity to speak with you today on the cybersecurity incident that affected the Internal Revenue Service (IRS) Data Retrieval Tool (DRT), specifically, the operational and cybersecurity decisions before and after the tool was taken offline. As the CIO, I embrace and support the Department's mission of *promoting student achievement and preparation for global competitiveness, fostering educational excellence and ensuring equal access*, by ensuring that we apply information technology (IT) effectively, efficiently, and securely. I take this responsibility seriously, and understand that this includes the entire Department, including Federal Student Aid (FSA) and all principal and support offices.

On March 3, 2017, I became aware that the IRS had confirmed that tax data accessed through the FAFSA DRT may have been used to fraudulently file tax returns. The Department's Security Operations Center (EDSOC) was notified about suspicious behavior on the IRS DRT on March 3, 2017. The DRT is an IRS tool leveraged by the Department's Free Application for Federal Student Aid (FAFSA) by allowing applicants to access required parts of their tax information

electronically for them to insert into their student aid applications. We immediately activated our incident response processes, beginning with actions to understand details of the events that occurred, and to identify appropriate responses. This involved coordination of Security Operations Center resources to gather forensic data and to gain a fuller understanding of the incident. We held daily meetings to facilitate communication between the technical staff of the Office of the Chief Information Officer (OCIO), FSA, and the IRS. Additionally, we reported the incident to our Office of the Inspector General and to the United States – Computer Emergency Readiness Team (US-CERT) at the Department of Homeland Security (DHS) on March 3, 2017, and March 4, 2017, respectively. While the Department's systems were involved, this was, in essence, a scheme directed at retrieving tax data from the IRS. The malicious actors used stolen PII to start FAFSA forms in order to obtain information from the IRS to attempt to file fraudulent tax returns. There is no evidence that the malicious actors were able to access any personal information held on the Department's systems. We are confident that the personal information the Department has on borrowers, students, and parents remains appropriately protected.

This issue, which involved the unlawful use of a Department system by outside parties, underscores the need for the Department to be continually vigilant in the operation and improvement of our cybersecurity capabilities. Toward that end, we have undertaken multiple projects to improve capabilities consistent with Industry Best Practices and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover). The Cybersecurity Framework applies the principles and best practices of risk management to improving the security and resilience of critical infrastructure. I will describe

several actions we have taken to further strengthen and enhance our cybersecurity program to protect sensitive data, including PII that is managed by the Department.

Incident Response

Incident response is a priority for the Department. In 2015 we created an Incident Response Planning Workgroup to address cybersecurity incidents and data breach response processes with separate work streams for communications, breach response planning, and privacy and legal. This group validated the mapping of key network systems, revised agency policies and directives as needed, evaluated and identified necessary amendments to the security clauses in vendor contracts, and developed technical and procedural protocols to guide decision-making in the event of a breach.

In Fiscal Year (FY) 2016, the Department conducted two incident response table-top exercises that helped us refine our incident response process through the development of lessons learned and identification of actions the Department needed to enhance our overall incident response processes. We have taken all actions identified in the two FY 2016 tabletops and plan multiple tabletops in FY 2017 as well.

Additionally, with the publication of the FY 2017 Inspector General Federal Information Security Modernization Act (FISMA) Reporting Metrics, the Department has performed a self-assessment against the Incident Response metric area. The Department is currently working to incorporate additional measures to achieve at least "Level 2" status across our Incident Response

program, to include the consolidation of our Security Operations Center capabilities, processes, and resources.

Internal Technical Controls

The Department has implemented a number of technical controls and solutions to detect policy violations, unauthorized changes, and unauthorized access to the Department's primary network. These include a Data Loss Prevention (DLP) solution, which went live in October of 2016 that restricts users from sending emails that contain sensitive PII, such as social security numbers, outside of the Department. In 2016 the Department also implemented Network Access Control (NAC), which allows for validation of the security posture of all endpoints against standard Department cybersecurity policies, and prevents the connection by any unauthorized device to the network. A third solution, Web Application Firewalls (WAFs), has been implemented and we are transitioning web portals and web applications to be protected by the WAFs.

The Department continues to focus on achieving Federal goals for strong authentication, as 100 percent of privileged users, and over 85 percent of our non-privileged users are required to use their Personal Identity Verification (PIV) card in order to log on to the Department's network.

Outreach and Collaboration with DHS

The Department has partnered with DHS on the implementation of automated solutions for Continuous Diagnostics and Mitigation (CDM), which will enable us to continuously monitor our network for intrusions and malicious activity. The Department also actively leverages DHS-provided shared security services such as EINSTEIN 3A tools for threat analysis and threat

indicators, US-CERT surge support for forensics analysis, and High Value Asset assessments.

The Department is also working in other ways to help ensure only authorized users are accessing the Department's systems and data. The FSA ID—a user-selected username and password—is required for students, parents, and borrowers to authenticate their identity and access their federal student aid information online. The websites that require an FSA ID to log in are fafsa.gov, NSLDS Student Access, StudentAid.gov, StudentLoans.gov, and the Federal Student Aid Feedback System (when a customer chooses to authenticate). Since the implementation of the FSA ID almost two years ago, over 45 million people have successfully created an FSA ID and have used their FSA IDs to log in over 315 million times. Recently the Department announced an additional disclaimer prior to log-in that will warn against unauthorized usage of the FSA ID by third-party for-profit entities. The user must select "Accept" in order to proceed.

While the Department has taken a number of positive steps to prevent the unauthorized access and loss of sensitive data, we recognize that there is still work to be done. The Department has fully embraced and is leveraging the mandates of the Federal Information Technology Acquisition Reform Act (FITARA), which we believe is prudent to continually improve and mature our processes in the realm of overarching IT Security and Governance.

Conclusion

I thank you for the opportunity to discuss the cybersecurity incident that affected the DRT, and the operational and cybersecurity decisions made before and after the tool was taken offline. The Department of Education and the IRS continue working together at all appropriate levels to

significantly improve the security and privacy protections around this important capability. I am confident that the technical solution currently being worked will achieve this goal. I would be pleased to answer any questions you may have.