Written Testimony of

Jason K. Gray
Chief Information Officer

United States Department of Education
Before the Subcommittee on
Government Operations of the
Committee on Oversight and Government Reform
United States House of Representatives

Thank you Chairman Connolly, Ranking Member Hice, and members of the subcommittee for this opportunity to appear before you today to talk about the progress the U.S. Department of Education (the Department) has made in implementing the Federal Information Technology Acquisition Reform Act (FITARA). I would also like to thank you for your continued support and commitment to improving Information Technology (IT) management across the Federal government.

The mission of the Department is to promote student achievement and preparation for global competitiveness by fostering educational excellence and ensuring equal access. As the Chief Information Officer (CIO), I embrace our mission and the responsibility to ensure that the Department is able to carry out that mission with the appropriate IT controls to ensure confidentiality, integrity, and availability.

I appreciate the support that I continue to receive from Secretary DeVos and Deputy Secretary Zais, as the Department would not have been able to achieve the improvements without their support. I also want to thank my colleagues in Federal Student Aid (FSA), the Assistant Secretaries, and everyone in the Office of the Chief Information Officer (OCIO) for their hard work and dedication. We could not have accomplished all that we have over the past four years without their support.

Institutionalization of FITARA at the Department of Education

Our journey began in 2015, with a comprehensive self-assessment to identify existing gaps in response to the Office of Management and Budget's (OMB) prescribed "Common Baseline," which outlines specific responsibilities and processes for the management of IT. That year, the Department received an overall grade of "F" for the FITARA 1.0 scorecard.

In late 2016, we began to implement a series of incremental changes to business processes and governance forums to realize our goals and objectives. Over the next two years, we continued to develop relationships across the Chief Executive Officer (CXO) community, improved and integrated our business processes, and focused on educating Department stakeholders. We made notable progress, which enabled us to improve on our FITARA 2.0 scorecard grade of "D" in May 2016 to a grade of "C+" for both the FITARA 3.0 (December 2016) and FITARA 4.0 (June 2017) scorecards. The Department continued to focus on improvements and achieved a grade of "B+" on FITARA scorecards 5.0 (November 2017), 6.0 (May 2018), 7.0 (December 2018), and 8.0 (June 2019).

In 2018, we increased our focus on ensuring that we had robust IT policies and governance processes in place to fully institutionalize FITARA within the Department. These incremental changes continued into 2019 and enabled the CIO to achieve unprecedented visibility across the Department's entire IT portfolio. In addition, the changes played a significant role in creating buy-in of key stakeholders for critical decisions involving the Department's effective acquisition, management, and use of IT resources to achieve the goals of FITARA. In late 2019, we were proud to see the results of our hard work lead to the Department achieving a grade of "A+" on the FITARA 9.0 (December 2019) scorecard.

Enterprise Oversight

In 2016, OCIO established a FITARA Implementation Working Group (FIWG), consisting of senior agency officials from the CXO community, including the Chief Financial Officer (CFO), the Chief Human Capital Officer (CHCO), the Chief Acquisition Officer (CAO), and the Federal Student Aid CIO to assist the CIO with overseeing the implementation of process-improvement initiatives. Through the FIWG, the Department has been able to establish the transparency and culture of collaboration needed to mature budget planning and execution, as well as acquisition planning and human capital management functions necessary for the effective management of the Department's IT resources.

The FIWG has been critical in assisting the CIO in formulating strategies and approaches to reach our FITARA maturity goals. The FIWG has provided oversight for the development and execution of over 70 maturity tasks for the practical implementation of FITARA. The FIWG continues to meet quarterly and is on the cusp of overseeing the completion of the final maturity tasks, Workforce Planning, and the review and approval of IT Acquisition Strategies and Plans.

In addition to the FIWG, we continue to leverage an integrated IT governance framework that promotes Department-wide participation and ongoing collaboration between OCIO and our CXO stakeholder communities. The framework strengthened the Department's IT investment management policies and processes in a number of ways. For example, it enabled us to refine our CIO risk-rating methodology for managing performance and assessing risk for major IT investments, and set forth more stringent criteria for evaluation and analysis to help promote data-driven decision-making to address competing priorities for IT resources. It also formed the basis for the design and implementation of a cradle-to-grave IT lifecycle management process that incorporates CXO functional areas into a streamlined governance process. The framework allows for the identification of efficiencies and redundancy in the IT portfolio.

These improvements have enabled the CIO to be directly involved in key decisions that may impact the Department's IT portfolio, our IT modernization initiatives, and our priorities.

Cybersecurity

Cybersecurity is another focus of FITARA, but it's also a priority for the Department. In 2017, OCIO developed a cybersecurity risk scorecard based on the National Institute of Standards and Technology (NIST) cybersecurity framework to improve our focus and alignment with OMB requirements for sound cybersecurity risk management practices. Since its inception, the Department has implemented several enhancements to drive measurable improvements to the cybersecurity posture of our information systems and make the scorecard an effective risk-management tool for Department stakeholders. For example, over the past year, we expanded the scorecard to include compliance with privacy laws and regulations and, in accordance with the President's Management Agenda, we incorporated metrics related to the accuracy, thoroughness, and timeliness of data.

The Department's holistic approach to enhancing cybersecurity is focused on providing the CIO, Department leadership, and system stakeholders with actionable information to make informed risk-based decisions. Through ongoing cybersecurity communication and education, and in leveraging the scorecard, the Department has seen continuous improvement in our ability to identify, prioritize, and mitigate risks. The scorecard has been a critical tool in driving conversations and accountability with vendors to further enhance the security of commercial off-the-shelf products and cloud.

Through these actions, we have continued to reduce cybersecurity risk empirically and demonstrably throughout the Department. As we mature our cybersecurity risk management approach, we're

ensuring alignment and integration with IT governance processes to inform current and future IT investment decisions.

IT Modernization

In my June 2019 testimony before this committee, I shared that the Department had just completed a massive IT modernization of our IT infrastructure. I also shared that the initiative transformed the way in which OCIO delivers IT services to the Department. This initiative involved migrating systems and over 450 terabytes of data into a secure cloud environment, upgrading approximately 5,000 laptops that significantly improved performance and enhanced employee productivity, and reducing the Department's network printers by 50% while replacing them with more secure personal identity verification (PIV) enabled printers, within an aggressive five-month period. In addition to reducing the Department's server storage costs from $1.43 per gigabyte (GB) to $0.12 per GB, the Department anticipates an overall cost saving of approximately $20.5 million over a 5-year period as a result of this modernization initiative.

While the Department may realize cost savings as a result of our IT infrastructure modernization, the true value was in our ability to quickly adapt and respond to the Department's needs throughout the Coronavirus pandemic. At the beginning of the pandemic, we were able to support a 100% remote workforce with minimal impact. When the PIV issuance process was suspended, we were able to quickly evaluate and implement, within days not months, an alternative solution to ensure compliance with federal requirements for network access, minimize risk to Department information and information systems, and enable the virtual onboarding of more than 300 new employees and contractors over the course of the pandemic, to date. In addition, operating in a true cloud environment, the Department was able to complete a massive technology refresh of twenty-eight major systems, more than 700 servers and over 500 terabytes of data, hosted in that environment over a single weekend with no impact to IT services.

The Department has also made significant investments in modernizing the way students, parents, and institutions of higher education, access and manage student aid, to improve our customers' digital experience, and enable us to be more responsive to their needs. Through the Next Generation FSA initiative, the Department is modernizing FSA's customer-facing digital platform and management of customer communications. This modernization initiative is on track to replace several older systems

related to application processing, partner participation, contact center management, and core processing.

The Department continues to make progress with the implementation of our five-year IT Modernization Roadmap that was originally developed in 2018. Through our IT governance processes, we've re-prioritized and made adjustments as appropriate to ensure that we can effectively support and ensure that the Department's operational needs are met.

Cost Savings

In 2019, we worked with stakeholders across the Department to develop innovative strategies focused on improving our ability to identify, track, and report cost-saving opportunities. As a result, we were able to assist program managers and business owners in identifying cost-saving initiatives, thereby increasing our cost-savings and avoidance targets by 105 percent over 2018 projections, allowing us to reallocate funding to critical resources required to enhance IT service delivery and improve the security of the Department's systems and data.

Performance Management and IT Workforce Planning

OCIO continues to work with the CHCO's office to assess and address the competency and skills gaps of the IT workforce. Critical to this effort is the identification and establishment of the requisite competencies to attract and maintain an IT workforce that meets our technology needs today and in the future. The Department is undertaking a number of efforts to reassess and mature both our IT staffing requirements and competency assessments of current IT staff.   In 2019, the Department completed competency models and assessments, and developed competency gap analysis reports. In 2020, the Department launched an agency-wide competency program focused on two functional areas, grants and IT. Through this initiative, the Department will identify IT competencies, create IT career and training maps, and identify a repeatable process for gap-closure assessments. The Department has also been fully engaged with the Department of Homeland Security, including the Cybersecurity and Infrastructure Security Agency, and NIST to ensure alignment with the National Initiative for Cybersecurity Education framework.

Opportunities for Continued Progress

While we have made significant strides in our FITARA maturation and IT modernization initiatives, the Department continues to seek Congress' assistance with the establishment of a Working Capital Fund for IT Modernization in accordance with the Modernizing Government Technology Act (MGT). The MGT provides the Department with the authority to establish the WCF but, unfortunately, we do not have the transfer authority necessary to activate the account. The Department coordinated with OMB and Congress to obtain appropriations language that would allow us to transfer funds to a WCF, and the President's Budgets for both 2020 and 2021 included that language. I respectfully request that Congress enact that language as soon as possible.

Conclusion

The Department's FITARA maturity is based not only on the establishment of the foundational policies and processes but on the Department's ability to truly leverage those policies and processes to make critical decisions. Ensuring that the CIO has a seat at the table and is directly involved in those critical decisions has enabled us to continue making progress towards our IT modernization goals.

Although we have made great strides towards institutionalizing FITARA within the Department, we will continue to assess and identify opportunities for improvement. I thank you for your time today and I look forward to your questions.