TESTIMONY OF
Beth Anne B. Killoran
Acting Chief Information Officer
U.S. Department of Health and Human Services
Before the
House Committee on Oversight and Government Reform
May 25, 2016

Good morning Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, thank you for giving me the opportunity to discuss federal information technology (IT). As the Acting Chief Information Officer (CIO) at the Department of Health and Human Services (HHS), my testimony will describe how HHS has been able to decrease the use of our end-of-life systems through a risk mitigation approach as well as discuss plans we have for remaining systems.

Leveraging IT to Support Mission Outcomes

HHS is the U.S. government's principal agency for protecting the health and well-being of all Americans and providing essential human services, especially for those who are least able to help themselves. IT is critical to enabling HHS to achieve its mission by fostering advances in medicine, public health, and social services. HHS spends approximately $5 billion annually to develop and maintain our IT. HHS has an annual operating budget of over $1 trillion, is responsible for almost a quarter of all federal outlays, and administers more grant dollars than all other federal agencies combined, including $7.3 billion in IT grants to state and local agencies for the procurement of IT to facilitate HHS programs.

In managing our IT programs, one of the key risks associated with operational systems is the ability to secure them. On this front, HHS has made measurable progress in improving cybersecurity. We are constantly making improvements resulting in our Federal Information Security Modernization Act (FISMA) score being the highest it has been in four years. Last year, our score improved by 23 percentage points from 35 percent in fiscal year (FY) 2014 to 58 percent in FY 2015.

Our work isn't done. HHS is continuing to strengthen our cybersecurity efforts. We are currently deploying the next phase of Einstein tools, defining the next generation of the Trusted Internet Connection, and deploying security monitoring tools consistent with the Department of Homeland Security's Continuous Diagnostics and Mitigation program. All of this work will not only strengthen our posture, but will build on HHS's Cyber Sprint by strengthening HHS's cyber infrastructure resiliency.

Finally, HHS has established the CyberCARE campaign to ensure HHS users are educated regarding cyber threats. The program won an annual award from the Federal Information Security System Educator's Association (FISSEA) and has been selected as a finalist in the Community Awareness category by U.S. Government Information Security Leadership Awards (GISLA). Each of these efforts illustrate that operational systems can provide continued mission support and functionality, if we continue to ensure they are secure and provide mission value.

Strategies and Capabilities to Modernize

When it is time to replace a legacy system, cloud capabilities reduce time necessary for modernizing or enhancing IT systems. By sponsoring cloud technologies through the federal standardized cloud products security assessment, authorization, and continuous monitoring process (FedRAMP), HHS works to offer and leverage cloud solutions. Cloud solutions have helped HHS reduce IT capital expenditures, reduce program risk, and reduce implementation time. Our most successful cloud implementation to date is development and modernization of the Department's financial systems. This ambitious program serves as a model on how to modernize IT infrastructure. As one of the largest federal financial systems upgrade to date, this program provides new capabilities across HHS through a shared delivery model utilizing a cutting-edge technology. In addition, HHS has successfully utilized cloud solutions to establish a new E-mail-as-a-Service (EaaS) platform, provide solutions to assist HHS in addressing urgent initiatives such as the Ebola response, and enhance communications through cloud technologies and business analytics. In each of these examples, cloud computing offerings have enabled HHS to reduce time to develop new products and services and increase collaborative capabilities.

Improving Our Program Management

Given the importance of IT, I have worked over the last year in my roles within the HHS CIO organization to improve our review process of our IT portfolios by conducting in-depth reviews of our own large IT programs. In collaboration with Operating Divisions to develop and implement a number of initiatives to address the most common systemic issues, we have improved transparency and enhanced governance.

Part of our FITARA change impacts how the HHS Office of the Chief Information Officer has evaluated the Department's major IT investments. Early CIO evaluations examined project management practices and operational performance placing an emphasis on timely reporting. I determined that we needed to enhance our evaluation model to adequately assess potential risks and dependencies. Implemented in October 2015, the revised risk model incorporates new risk factors, operational performance metrics, and is scored based on OMB's 5-point risk scale.

In addition, HHS closely monitors IT investment risks and quickly identifies mitigation strategies for reducing risk. If a major system is identified as "High Risk" for three consecutive months, then either the HHS or Operating Division Chief Information Officer requires that a TechStat is conducted. A TechStat is a face-to-face, evidence-based review of an IT program, undertaken with agency leadership, powered by the IT Dashboard. HHS has a robust TechStat program that is valuable for both developmental and operational programs. In FY 2015, HHS performed eight TechStat reviews of IT investments in the HHS IT Portfolio to reduce the risk associated with these investments.

TechStats have been performed on both of the programs cited in the GAO legacy systems. In June 2013, a TechStat was conducted on the first program identified by GAO, the Medicare Appeals System (MAS). The MAS supports a tracking system for Medicare appeals across all Medicare programs (fee-for-service, Medicare Advantage, and Part D). The TechStat review identified additional project management best practices that should be implemented to track schedule and cost changes. Based on the review, the Centers for Medicare & Medicaid Services implemented those recommendations resulting in the program now consistently receiving the lowest risk rating.

The Trusted Internet Connection (TIC) went into operations and maintenance in 2015 after we completed installation on our final three locations. The final phase ensures that all HHS traffic is routed through centralized access points, increasing visibility of network traffic and reducing vectors for compromise and attack. To strengthen the program as it continues to make changes, a TechStat was performed for the Trusted Internet Connection (TIC) in February 2016. That TechStat identified program practices regarding performance metrics and reporting that needed to be added to monitor progress. Since the TechStat review, my team has implemented several initiatives to collect, analyze, and report performance metrics, resulting in reducing the program risk level. In addition, the TIC has performed a number of modernization activities this year and more will continue over the next 12-18 months.

Developing Our Staff

As we continue to enhance our risk management practices this year, we will continue to focus on preventing investments from trending as high-risk by working with project managers to solve potential problems before they become issues. We work on a one-on-one basis with project managers in order to ensure that program health is optimized and appropriately represented. Through our outreach efforts, we have found that investing in our most important resource, our people, is critical to ensuring the health of our IT portfolio.

We are committed to providing training for our IT program and project managers. To improve the probability of program success, our training program aligns with the Office of Federal Procurement Policy’s October 2009 guidelines and standards. HHS provides three levels of training (entry, mid, and senior level) for IT program and project managers to receive certification as a Federal Acquisition Certification program professional. HHS has trained close to 300 IT program and project managers since November 2015. This was accomplished through a combination of classroom and virtual project managers collaboration network where practicing can collaborate, discuss best practices, share innovative ideas and learn from each other. In addition, HHS has sponsored an agency Annual IT Project Manager Summit for the last three years where the entire HHS IT community comes together to strategize, share insights on improvement strategies that are working well, not only at HHS but the federal government, and to participate in training.

Beyond development, HHS is working to attract new IT staff to critically important positions for our long-term success. Over the past two years, we developed the HHS IT Human Capital Strategy pilot for Cybersecurity, an approach that outlines IT career paths and enables us to establish a professional continuum that defines competencies employees need to advance their career. We are currently working to expand this program to other IT professions. Partnering with the Office of the Chief Human Capital Office, we are working to identify new methods for recruiting critical IT positions through direct hire, internships, Schedule A, and targeted recruiting through universities and professional organizations by marketing our Department’s mission to draw professionals to a career at HHS.

Making the Case for Change

Like other federal agencies, HHS spends significantly more on operations and maintenance than on DME. HHS recognizes the need for greater development spending, and modernizing or replacing unsupported technology, but challenges to this practice exist. Some of our specific challenges include lack of clear authority to require grantees to replace or modernize their systems, DME funding used for new mandates, and interdependencies of systems or software that prohibits changes. To make the case for funding, agencies must first identify which IT investments qualify as legacy, and then prioritize programs. For example, HHS would not consider an IT system that entered operations and maintenance last year, such as the TIC nor would a decade old system with underlying technology still supported by the manufacturer (MAS) be considered legacy. Once a program has been identified as needing replacement, agencies will need adequate funding to make legacy system changes.

One way to address the Government funding challenge is by Congress passing the Administration's proposed $3.1 billion IT Modernization Fund (H.R. 4897). The IT Modernization Fund would serve as a mechanism for agencies to upgrade legacy IT to more modern, cloud-based systems. To ensure agencies are modernizing the most critical systems, the legislation would establish a board of experts to help prioritize high-risk federal systems for replacement. The board would also look for multiple legacy systems that could be replaced with a few common platforms.

Congress established the Nonrecurring Expense Fund (NEF) at HHS, which permits HHS to procure capital acquisitions including IT and facilities infrastructure necessary for operation of the Department. These funds provide vital support to HHS. This funding has supported a number of critical IT system modernizations. For example, in FY 2014, HHS allocated NEF funds to invest in an electronic case processing system for the Office of Medicare Hearings and Appeals, modernization of the Resource and Patient Management System in the Indian Health Service, and the Centers for Disease Control and Prevention performed IT infrastructure enhancements to public health programs. Since the NEF was established, HHS has used this resource to provide support to critical Department-wide cybersecurity efforts, including activities to address emerging issues, which were then able to be urgently addressed. The NEF helps HHS meet both long-term IT procurement needs and address the needs of a rapidly changing cybersecurity environment, but could additionally benefit from ITMF. Without these types of funds, HHS would struggle to make necessary modernizations to keep our IT systems current and secure.

The NEF also enabled the successful financial systems modernization effort I mentioned at the outset of my comments today. The NEF is an important funding source for large-scale projects to modernize systems, improve the underlying infrastructure, and leverage new technology. These are the types of projects that can drive transformational change, improve mission delivery, effectiveness, and efficiency. More importantly, these are the types of projects that address the risks associated with operating on outdated and unsupported platforms.

Simply put, the cost of doing nothing is not nothing. As systems age, the risks to security, reliability, and availability are very real – increasingly so these days, as attempts to exploit system vulnerabilities become more sophisticated. HHS's financial systems and other IT systems have benefitted from NEF funds.   Given the scale of HHS's operations and the scope of its programs, the implications of a system breach or failure represent risks that are difficult to quantify.

Understandably, HHS's front-line programs receive much visibility– these are important programs, after all they touch and improve the lives and well-being of countless Americans. It is imperative to recognize, however, that these programs cease to operate effectively and efficiently without a secure and reliable IT infrastructure supporting them. The NEF and the ability to use those funds effectively, addressing the Department's most pressing business needs, supports the sustainability of HHS's IT environment and HHS's mission. I thank you for your continued support and authorization of these essential dollars.

Conclusion

HHS recognizes that IT investment planning and management is a dynamic and fluid process that occurs at multiple levels. IT investments must be selected with involvement of key stakeholders and with the understanding of mission risk. Once selected, IT investments must be continually monitored and evaluated to ensure that each approved IT investment effectively and efficiently supports the agency mission.

The federal government, through adoption of the IT Modernization Fund, has the ability to make meaningful changes to IT legacy systems and measurably improve the mission and business effectiveness of the federal government. My comments today have highlighted this impact at HHS – from developing a strategic approach to comprehensively modernizing HHS's IT portfolio, to managing these large, complex initiatives and being effective stewards of the funds entrusted to the Department, to enabling improved mission delivery supported by a secure, reliable, and high-performing IT environment. It is a track record I hope to build on, working with you and your Congressional colleagues on future endeavors. Thank you for the opportunity to speak with you today and I look forward to answering your questions.

Beth Killoran
Acting Chief Information Officer
Acting Deputy Assistant Secretary for Information Technology
Office of the Chief Information Officer

In October 2014, Ms. Beth Killoran joined the Department of Health and Human Services. Since December 2015, she has served as the acting Deputy Chief Information Officer. As acting CIO for the Department of Health and Human Services, she provides leadership on high priority projects, engages in strategic IT investment planning, and drives change across the organization. Prior to this role she served as the Acting Deputy Chief Information Officer (April 2015-December 2015) and as the Executive Director for the Office of IT Strategy, Policy and Governance.

Before to joining HHS, she served 11 years at the Department of Homeland Security in a number of leadership roles throughout the organization including Under Secretary for Management, Office of the Chief Information Officer, Citizenship and Immigration Service and Customs and Border Protection. Over the course of her DHS career, Beth served in positions covering investment management, risk management, and program management of the DHS acquisition portfolio and IT investments totaling over $18 billion.

Finally, Beth served 9 years at the Department of the Treasury where she provided IT infrastructure support and operations for over 20,000 employees across 1,500 locations. During her tenure, she provided IT operational support in response to the 9/11 and Oklahoma City bombing events.

Beth holds a Master of Science in Technology Management from University of Maryland and a Bachelor of Arts in Psychology with a certificate in Personnel Management from the University of Maryland Baltimore County.