S. Hrg. 118–152

SECURING THE NATION: MODERNIZING DHS'S MISSION–CRITICAL LEGACY IT SYSTEMS

HEARING

BEFORE THE

SUBCOMMITTEE ON EMERGING THREATS AND SPENDING OVERSIGHT

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

MAY 31, 2023

Available via the World Wide Web: http://www.govinfo.gov

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PUBLISHING OFFICE
52–438 PDF WASHINGTON : 2023

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware	RAND PAUL, Kentucky
MAGGIE HASSAN, New Hampshire	RON JOHNSON, Wisconsin
KYRSTEN SINEMA, Arizona	JAMES LANKFORD, Oklahoma
JACKY ROSEN, Nevada	MITT ROMNEY, Utah
ALEX PADILLA, California	RICK SCOTT, Florida
JON OSSOFF, Georgia	JOSH HAWLEY, Missouri
RICHARD BLUMENTHAL, Connecticut	ROGER MARSHALL, Kansas

DAVID M. WEINBERG, *Staff Director*
ZACHARY I. SCHRAM, *Chief Counsel*
WILLIAM E. HENDERSON III, *Minority Staff Director*
LAURA W. KILBRIDE, *Chief Clerk*
ASHLEY A. GONZALEZ, *Hearing Clerk*

SUBCOMMITTEE ON EMERGING THREATS AND SPENDING OVERSIGHT

MAGGIE HASSAN, New Hampshire, *Chairman*

KYRSTEN SINEMA, Arizona	MITT ROMNEY, Utah
JACKY ROSEN, Nevada	JAMES LANKFORD, Oklahoma
JON OSSOFF, Georgia	RICK SCOTT, Florida

JASON M. YANUSSI, *Staff Director*
ALLISON M. TINSEY, *Senior Counsel*
SCOTT MACLEAN RICHARDSON, *Minority Staff Director*
MARGARET E. FRANKEL, *Minority Professional Staff Member*
KATE KIELCESKI, *Chief Clerk*

CONTENTS

WITNESSES

WEDNESDAY, MAY 31, 2023

ALPHABETICAL LIST OF WITNESSES

APPENDIX

SECURING THE NATION: MODERNIZING DHS'S MISSION–CRITICAL LEGACY IT SYSTEMS

WEDNESDAY, MAY 31, 2023

U.S. SENATE,
SUBCOMMITTEE ON EMERGING THREATS AND
SPENDING OVERSIGHT,
OF THE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10:15 a.m., in room SD–562, Dirksen Senate Office Building, Hon. Maggie Hassan, Chairwoman of the Subcommittee, presiding.

Present: Senators Hassan [presiding], Sinema, Rosen, Ossoff, Romney, Lankford, and Scott.

OPENING STATEMENT OF SENATOR HASSAN[1]

Senator HASSAN. This hearing will come to order.

Good morning and welcome to our distinguished panel of witnesses. Thank you for appearing today to discuss the Department of Homeland Security's (DHSs) reliance on aging information technology (IT) systems as it works to secure the Nation, and why it is crucial that the Department and its component agencies modernize their mission-critical systems.

I also want to thank Ranking Member Romney and his staff for working with us on this hearing and for our continued partnership to address emerging threats and reduce wasteful government spending.

Today's hearing continues our Subcommittee's work to replace aging government technology that wastes taxpayer dollars, undermines our security, and limits government's efficiency and responsiveness. As our Subcommittee continues to encourage agencies to adopt modern systems that are more efficient, more cost effective, and frequently more capable, we will hear today from senior DHS officials about their outdated technology negatively impacts the Department's budget and our nation's safety.

For example, if an aging system that DHS uses to vet passengers or visitors traveling into or through the United States goes offline there is a chance that a dangerous person could enter our country. In such cases, workarounds can help limit national security risks, but they can also cause commercial delays or miss real-time intelligence.

[1] The prepared statement of Senator Hassan appears in the Appendix on page 25.

The Government Accountability Office (GAO) and the DHS inspector general (IG) have assessed DHS's IT modernization efforts and in doing so have raised concerns about its reliance on outdated IT systems that perform mission-critical operations. They have looked at DHS IT systems that ensure the security of air travel, support disaster mitigation and preparedness activities, and enhance border security, and they have asserted that the failure of any of these systems would have a significant impact on public safety and national security. That is why it is crucial that DHS modernize these systems.

Today's hearing is an opportunity to examine how legacy information technology is a threat to national security and how DHS can responsibly update its systems. I look forward to hearing from all of our witnesses about the risks posed by legacy IT systems at DHS and how DHS can successfully modernize these systems to keep the American people safe, secure, and free.

I will now recognize Ranking Member Romney for his opening remarks.

OPENING STATEMENT OF SENATOR ROMNEY[1]

Senator ROMNEY. Thank you, Madam Chair. I appreciate the opportunity to hear from the witnesses today. In the interest of time I am going to ask for my comments to be included in the record.

I would note that the vulnerability of our systems has obviously changed in dramatic ways with the advent of artificial intelligence (AI). There are probably two sides of that issue, which is, one, we are more vulnerable, but two, the capacity to update systems through the use of AI to do some software development is probably enhanced. How this will change our perspective I think is one of the topics we should discuss today.

But I think we all recognize that intrusion into government systems is a risk. It has been carried out a number of times by the Chinese or by their cohorts and by Russians, and we need to take special care to protect the information provided by the American people.

With that I will turn to the questions that we have and the testimony of our witnesses.

Senator HASSAN. Thank you very much, Senator Romney.

It is the practice of the Homeland Security and Governmental Affairs Committee (HSGAC) to swear in witnesses. If you will all please stand and raise your right hands.

Do you swear that the testimony you give before this Subcommittee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. HYSEN. I do.

Mr. ARMSTRONG. I do.

Mr. OSHINNAIYE. I do.

Mr. WALSH. I do.

Senator HASSAN. Thank you. Please be seated.

Our first witness today is Eric Hysen. Mr. Hysen serves as the Chief Information Officer (CIO) for the Department of Homeland Security. He is responsible for strategically aligning the Depart-

[1] The prepared statement of Senator Romney appears in the Appendix on page 26.

ment's technology resources to support DHS's missions and activities. He was a founding member of the U.S. Digital Service (USDS) at the Office of Management and Budget (OMB) and worked as a software engineer for Google before joining the Federal Government.

Welcome, Mr. Hysen. You are recognized for your opening statement.

TESTIMONY OF ERIC HYSEN,[1] CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. HYSEN. Chair Hassan, Ranking Member Romney, and distinguished Members of the Subcommittee, thank you for the opportunity to testify today.

The Department of Homeland Security interacts with the American people on a daily basis more than any other Federal agency, from travelers moving through our air, land, and sea ports, to businesses importing goods into our country, to disaster survivors applying for assistance in their hour of need.

An increasing portion of these interactions occur through our information technology systems. Modernizing our legacy IT systems is essential to improving the experience of those that rely on our department for critical services and of strengthening our ability to carry out our vital homeland security missions. Modernization further offers opportunities to strengthen our cybersecurity posture and reduce spending.

I have worked to improve service delivery at all levels of government throughout my career. As you noted, Chair, I worked in Silicon Valley as an engineer and product manager to launch tools in over 30 countries to help people vote and engage with their representatives. I worked in philanthropy and State government to improve social service delivery at the State and local level. I left the private sector to cofound the United States Digital Service, where I worked to improve key services across DHS, and I bring those perspectives to my current role as the Department's Chief Information Officer.

Historically, agencies across the Federal Government, including DHS, took a "big bang" approach to IT modernization. At its most basic level, we attempted to acquire and deploy IT systems in the same way that we acquire and deploy ships. Government staff spent years gathering requirements, awarding a large contract to a single system integrator to build to those exact requirements, extensively test against them, and then launch. In theory, everything would go well, the new system would replace the old one, and then go into ongoing maintenance for several years until it was time to start the entire process over and modernize again.

In practice, however, this approach, known as "waterfall" software development, leads to modernization programs going over budget and behind schedule at alarming rates. Single, "big bang" releases of new systems lead to massively increased risk.

At DHS today, we reject this approach in favor of a more incremental, iterative, and measured strategy based on private sector best practices that enable us to successfully modernize key services

[1] The joint prepared statement of Mr. Hysen appears in the Appendix on page 27.

and retire costly legacy systems. Our newly initiated modernization programs focus on defining a minimum viable product, initial functionality that can be launched within months, not years. From there, we follow an agile software development methodology that gathers requirements, builds, tests, and launches software, in rapid, iterative cycles. Modernized systems are deployed and implemented in parallel to the old legacy ones, to buy down risk over time.

For our existing modernization programs, started under the old model, we are focused on transitioning as much of the work to the new approach as possible. A critical element of this approach is that government, not any one vendor, must serve as the integrator ultimately responsible for successful delivery of an IT system. We depend on our industry partnerships but require strong technical expertise in Federal service to oversee contracts and ensure results. I am focused on strengthening our IT workforce to enable this, both by bringing in talent from the private sector and creating new opportunities for our workforce to develop and gain new skills.

Our written testimony provides examples of our transition of legacy modernization programs into this new approach as well as of newer initiatives started under this model.

This work is showing results in strengthening cybersecurity, reducing spending, and most importantly, improving customer experience. Just yesterday we announced that the Department had reached its target of eliminating 20 million of the 190 million hours of administrative burden that we place on the public each year through modernizing our IT systems and simplifying our services.

We still have much work to do, but I am proud of the work done by my colleagues here today and the entire DHS IT community to deliver modernized, secure, effective, and usable systems to support our Department's critical missions.

Thank you again for the opportunity to testify today, and I look forward to your questions.

Senator HASSAN. Thank you very much.

Our next witness is Charles Armstrong. Mr. Armstrong serves as the Chief Information Officer for the Federal Emergency Management Agency (FEMA). His role is to ensure that the agency's technology can support its mission to prevent, prepare for, and recover from domestic disasters. He previously served in the Customs and Border Protection (CBP) Office of Information and Technology and was Deputy Chief Information Officer of DHS.

Welcome, Mr. Armstrong. You are recognized for your opening statement.

TESTIMONY OF CHARLES R. ARMSTRONG,[1] CHIEF INFORMATION OFFICER, FEDERAL EMERGENCY MANAGEMENT AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. ARMSTRONG. Thank you. Good morning Chair Hassan, Ranking Member Romney, and distinguished Members of the Subcommittee. Thank you for the opportunity to testify today in support of the agency's information technology modernization program.

[1] The joint prepared statement of Mr. Armstrong appears in the Appendix on page 27.

FEMA is utilizing an agile development and delivering small segments and providing an opportunity for customers to interact with systems in a rapid fashion. This approach allows our developers to receive real-time feedback from customers on their experience.

FEMA requires continuous modernization to maintain mission readiness. The overarching goal is to modernize and streamline processes through the consolidation of systems and platforms. As Stafford Act-related disasters increase, our system must be able to scale to support the magnitude of the disaster.

Today I will highlight three FEMA modernization programs: Grants Management Modernization (GMM), the National Flood Insurance Program (NFIP), and Individual Assistance (IA). First, let me begin with Grants Management.

Based on prioritizing customer experience, FEMA is consolidating eight disparate legacy systems into the FEMA Grants Outcomes (FEMA GO) System. The new IT platform is targeted toward the entire grants community of users, including FEMA personnel, the grants recipients, the sub-recipients across State, local governments, Tribal, and territorial partners. GMM, through FEMA GO, has migrated 5 programs to the new system in fiscal years (FY) 2018 through 2022, and has on boarded 14 additional grant programs in fiscal year 2023. FEMA plans to onboard approximately 20 additional grant programs by April 2024, and decommission all the old systems by 2025.

Next I am going to discuss the National Flood Insurance Program, or the Pivot system. As a goal for making wise land use decisions, Congress established the NFIP to encourage communities to enact floodplain management ordinances consistent with Federal standards. Pivot facilities and consolidates the NFIP core business processes from the legacy system and services program. Pivot was an agile modernization program in the newer mold of technology modernization, replacing the old NFIP system and services program.

Pivot processes millions of transactions of flood insurance applications, policies, and claims, and provides business workflow to automate manual processes and provides reporting and data analytics for financial and business requirements. Pivot met its full operational capability in October 2020, ahead of schedule and under budget.

Finally, the Individual Assistance Technology Support Services program. FEMA is planning to migrate 9 disparate systems into the Individual Recovery Information System (IRIS), and will be replatforming into the recovery cloud environment. The IRIS full operational capability is projected for July 2027, contingent on out year funding. FEMA's Individual Assistance also implemented Login.gov as a multifactor authentication and to support State, local, and Tribal access in 2023, and plans to place this integrated component in the beginning of the registration intake process once streamlined disaster assistance intake is rolled out in August.

In closing, again, FEMA thanks the Committee for the opportunity to be a witness at today's hearing. The agency looks forward to continued partnership and is open to any questions that you may have. Thank you.

Senator HASSAN. Thank you, Mr. Armstrong.

Our third witness is Yemi Oshinnaiye. Mr. Oshinnaiye is the Chief Information Officer for the Transportation Security Administration (TSA). He works to ensure that TSA's technology capabilities meet the agency's task of keeping highways, railroads, mass transit, and air travel safe. He previously served as the Deputy Chief Information Officer at U.S. Citizenship and Immigration Services (USCIS).

Welcome, Mr. Oshinnaiye. You are recognized for your opening statement.

TESTIMONY OF YEMI OSHINNAIYE,[1] CHIEF INFORMATION OFFICER, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. OSHINNAIYE. Good morning, Chair Hassan, Ranking Member Romney, and distinguished Members of the Subcommittee. Thank you for the opportunity to appear before you today and discuss the modernization of DHS's critical legacy IT systems.

I have the honor of serving as the CIO for TSA. In this role, I am responsible for technology management, including technology delivery and support, innovation, cybersecurity, and all facets of IT resourcing that TSA uses to enable its mission. Prior to TSA, I served as the Deputy CIO for the U.S. Citizenship and Immigration Services, where I led innovative practices and solutions to address the challenges of legacy systems and the processes used to modernize them. These practices are still in use today, to enable modern systems and continue innovation for the nation's immigration benefit system and across Federal Government.

Prior to my Federal service, I worked as a Chief Technology Officer in the private sector, and as an entrepreneur, providing software development and systems engineering services.

At TSA, we are responsible for the security of over 430 Federalized airports, and routinely screen more than 2 million passengers, 5 million carry-on bags, 1.4 million pieces of checked luggage daily for explosives and other prohibitive items.

TSA IT systems enable TSA to provide world-class security for the American traveling public while ensuring confidentiality, integrity, and availability of TSA data and resources. I am proud of how TSA is approaching modernization to ensure our infrastructure, systems, and IT solutions remain resilient and effective.

Our strategy for modernization at TSA is in line with the DHS overall approach. Our focus is on leveraging human-centered design for problem-solving technique we use to engage our customers. This technique allows us to leverage user experience and incorporate this feedback into our overall modernization strategy. When we operate this way, we provide a better opportunity for the user community to influence the final product, which improves the final product.

TSA's IT modernization strategy enables the agency to use outsourced, critical portions of the modernization to industry partners, such as cloud vendors, who invest heavily in modern services and infrastructure. Leveraging this investment empowers TSA to

[1] The joint prepared statement of Mr. Oshinnaiye appears in the Appendix on page 27.

focus more of our talent and resources on process improvement and strategies for continued mission success.

Two great examples of this are the Performance and Results Information System (PARIS). This system manages compliance and inspection activities. We recently successfully migrated to the cloud platform which enables us to grow, scale, and provide robust analytics for TSA compliance activities.

Another example is the Mission Scheduling Notification System (MSNS). This system scheduled Federal air marshals to protect inflight travel. MSNS is a collection of systems with integration to many other systems, but currently includes a lot of extensive manual processing. We prototyped the modern process using cloud platforms with an intuitive design in a matter of months using agile, that alleviates manual processing. Our solution delivers rapidly over time by taking an iterative approach.

These two examples show how TSA IT delivers effective technology to the mission and the strategy to sustain its capability.

Chair Hassan, Ranking Member Romney, and distinguished Members of the Subcommittee, thank you for the opportunity to testify before you today and for your continued support of TSA. I look forward to this discussion and your questions.

Senator HASSAN. Thank you very much.

Our final witness is Kevin Walsh. Mr. Walsh is the Director of the Government Accountability Office's Information Technology and Cybersecurity reviews. He has led GAO's work to identify challenges associated with the Federal Government's use of aging technology, coordination of IT acquisitions, and IT-related risk assessments. His work has specifically focused on making recommendations to improve DHS's IT systems.

Welcome, Mr. Walsh. You are recognized for your opening statement.

TESTIMONY OF KEVIN WALSH,[1] DIRECTOR, INFORMATION TECHNOLOGY AND CYBERSECURITY, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WALSH. Chair Hassan, Ranking Member Romney, and Members of the Subcommittee, thank you for inviting GAO to testify on this important issue.

As you have heard, DHS plays a pivotal role in safeguarding the United States and its citizens from a variety of threats, and its IT systems are critical to that mission. Among other things, DHS prevents and responds to acts of terror, its IT systems help to coordinate intelligence gathering and analysis, secure transportation systems, and collaborate with Federal, State, and local law enforcement. DHS also secures our borders. This technology has intercepted illegal activities, combats human trafficking, and identifies unauthorized individuals, illicit drugs, and contraband.

DHS also protects our infrastructure. Its IT defends against cyber threats to our essential services, sensitive information, and national security. DHS also responds to natural disasters. Its tech coordinates our emergency response, supports affected communities, and aids in their eventual recovery.

[1] The prepared statement of Mr. Walsh appears in the Appendix on page 37.

In 2023, the Department expects to spend about $10 billion on IT. Operating and maintaining existing systems is about $9 billion of that. In many cases, those existing systems are not the newest. However, because they are old does not mean they are at risk or in need of retirement. The systems to focus on are those that we would flag as legacy IT, systems that are outdated or obsolete that may have heightened security risks or are not meeting mission needs.

Worryingly, the Department's efforts to modernize such systems have a history of costing more than planned and taking longer than promised. We have reported that the Department is on its third attempt at modernizing its financial systems, which recently breached schedule and performance goals. Its biometric identity management services, handling fingerprinting and facial recognition, are outdated, and the replacement project is years behind schedule. The system it uses to award billions in grants to prepare and respond to disasters is also outdated, and the replacement project is also years behind.

While all is not quite right in the Land of Oz, DHS has been taking promising steps to address these issues. For example, they have halted or suspended projects that are going poorly, they have addressed our recommendations at a better-than-average rate, documented lessons learned, and used modern development technologies like agile and incremental. They have also been working diligently to address the associated high-risk area on IT and financial management functions.

Going forward, DHS needs to continue addressing its legacy systems, cataloging those systems, identifying what is not performing, and prioritizing the work ahead. They should also make sure to turn off the old systems.

It is worth noting that this should not be a one-time effort. It should be part of every agency's portfolio management to consider what IT is not doing well. Ideally, we should also be forecasting when this will occur so that the government's responses are proactive instead of reactive. The Chair's Legacy IT Reduction Act includes provisions along those lines.

Finally, this probably is not what you want to hear, given the current fiscal environment. However, modernization may not be a cost-saving endeavor. What we do get are newer systems that are more efficient, with better functionality, and stronger security.

This concludes my statement, and I look forward to your questions.

Senator HASSAN. Thank you, Mr. Walsh. We will now proceed with our first round of questions, and I will start with a few and then turn it over to the Ranking Member.

The first question is to you, Mr. Walsh. This Subcommittee has led efforts to save taxpayer dollars by encouraging agencies to modernize their outdated and obsolete IT systems. These aging systems not only increase costs, they can also jeopardize our national security.

What specific risks has GAO identified that are presented by DHS's aging IT infrastructure, and can you provide an example, please.

Mr. WALSH. The general risks to running legacy systems are risks to your security, mission needs, staffing, and cost. In a specific example, as has already been mentioned, FEMA is working on its Grants Management modernization program. That program is to replace a series of legacy systems that currently are experiencing the problems we are describing today. They have manual processes that are a burden for recipients, a burden for the agency, and are slowing down the response to disasters. If that legacy system were to fully go off the rails, a disaster without grants from the government would be very difficult for our citizens.

Senator HASSAN. Thank you. This is a question to Mr. Hysen and to Mr. Walsh. It is deeply concerning that DHS relies on outdated technology for some of its most important work. I heard the testimony about progress you are making, but there is still really important work where we are using outdated technology. Mission-critical systems should be an IT modernization priority, but different agencies have different ideas about what makes an IT system mission critical.

Mr. Hysen, how does DHS currently prioritize which systems to modernize?

Mr. HYSEN. Chair, thank you. As we look at establishing modernization priorities we are looking to those that fit into three categories, those that present significant cybersecurity risk, those that present opportunities to improve the experience the public has interacting with DHS services, and those that present opportunities to improve how our employees do their job every day and enable them to do that more effectively.

On the cyber front, one tool that we have developed to aid us in this is a unified cybersecurity maturity model that evaluates all of our IT systems across the Department on a number of different cyber axes, and enables us to best identify areas of risk to prioritize our modernization efforts.

Senator HASSAN. Thank you. Mr. Walsh, what is GAO's criteria for determining if something is mission critical?

Mr. WALSH. We have a two-tiered test. The first looks at whether the functions of a given system are unique to the agency. If it is unique, then any sort of damage or disruption, what kind of impact it would have to the mission of that agency.

Second tier, systems who, if they were damaged or the data were lost, misused, or disclosed, would have a debilitating impact upon the agency.

Senator HASSAN. OK. Mr. Hysen, could DHS adopt GAO's mission-critical criteria to help decide what IT modernization projects to prioritize?

Mr. HYSEN. Absolutely, Chair, and I believe we look at very similar criteria across our planning efforts.

Senator HASSAN. I think it is a really important area to focus on and really try to make sure that that is, in fact, how the agency is approaching it.

Mr. Oshinnaiye and Mr. Armstrong, a question for the two of you. Let us discuss a couple of examples of systems that are critical to DHS's mission but rely on aging technology. Since 2009, TSA has used the Secure Flight System to spot potential threats to commercial airline travel within and outside of the United States. This

system connects to many other agency systems to identify individuals who are ineligible to fly.

Mr. Oshinnaiye, can you walk us through what would happen if the Secure Flight System were to go offline, fail, or be even partially inaccessible?

Mr. OSHINNAIYE. Thank you, Chair. Similar to what Mr. Walsh said, the system has been in existence for a while, but calling it a legacy system would not be the same as a mainframe. That system is constantly updated, and if that system would go offline we do have an offline policy or process where we can operate for a certain amount of time. We also test that scenario for COOP, to make sure that if we did have an outage we would still be able to operate and protect travelers.

Senator HASSAN. But what would happen? I understand there is a workaround, and I made that comment in my opening, but a workaround has its costs too. What, if it were to go offline, or fail, or be even partially inaccessible, and let's say your workaround did not work, what happens?

Mr. OSHINNAIYE. In a catastrophic event or if you would exceed the COOP timeframe, it would hinder our ability to see travelers who are dangerous to other travelers.

Senator HASSAN. OK. Thank you.

Another example of DHS's aging IT infrastructure is FEMA system that enables the flows of funds and services to disaster survivors, and Mr. Walsh was just getting at that. Mr. Armstrong, if this system went down, how would Americans in need because of a natural disaster, access FEMA services?

Mr. ARMSTRONG. Chair Hassan, can I ask to clarify that, because Mr. Walsh talked about Grants Management, and I want to make sure you are not referring to Individual Assistance.

Senator HASSAN. Let us talk about Individual Assistance. What would happen, in a natural disaster, access to the Individual Assistance system goes down?

Mr. ARMSTRONG. Individual Assistance, as you can imagine, is critical to the mission of FEMA. It is one of the systems that we rely on to give immediate recovery to that survivor during the recovery and response period of a disaster. Without that capability in place we would have to resort to manual processes, which could either slow things down or prevent us from adequately addressing the needs of the individual during that critical time.

Senator HASSAN. It could have a really significant, and at times, really dangerous impact, right?

Mr. ARMSTRONG. Yes, ma'am.

Senator HASSAN. Thank you.

I will now turn to Senator Romney for his questions.

Senator ROMNEY. Thank you, Chair. I appreciate the chance to listen to each of you and to hear your perspectives and update on our systems. I am curious, as we begin, Mr. Hysen, do Mr. Armstrong and Mr. Oshinnaiye both report to you? What is the organizational structure within DHS for the various agencies that are part of the entire entity?

Mr. HYSEN. Thank you, Ranking Member. Under the Federal IT Acquisition Reform Act (FITARA), the component CIOs under DHS

report in to me. However, they also maintain a reporting structure into their component agencies.

Senator ROMNEY. It is a matrix reporting system. Do they follow the same approach that you described? I am curious as to how widespread your approach is, which, as you described, I will call it the "big bang" approach, which is a big contract going out and waiting for a full system being delivered by an outside contractor, versus something now which I do not know how you would describe it incremental, which is you begin with a system and then add onto it as time goes on, improve it as time goes on.

How much of what is being done follows the latter approach as opposed to the former "big bang" approach?

Mr. HYSEN. At this point, Ranking Member, agile delivery and this newer approach to modernization is widespread across DHS. This has been a journey over really the last decade. Some of our component agencies were earlier adopters of this approach, some have made that transition more recently, but it is now the norm.

Senator ROMNEY. Do you know whether that is the case also more broadly through our government? I presume you interact with CIOs in other departments as well. Is the agile approach being adopted on a widespread basis?

Mr. HYSEN. I believe so. That has been a transition that has been discussed across the Federal CIO council and among my colleagues over the last many years.

Senator ROMNEY. We have a history of spending a lot more than the private sector to get an updated modernization of our systems. Is that because of the prior approach, or is it just endemic to the way government works?

Mr. HYSEN. I believe it is, in many ways, tied to that approach. One of the results of that "big bang" approach with single-system integrators was that every IT system would build everything from the ground up. They would have their own infrastructure, their own support teams, their own log-in systems, for example. As we have moved to modernize, we are looking to break that down, offer up common enterprise services for common pieces of functionality—that was the norm, for example, when I worked in Silicon Valley—and enable each individual system to only focus on their unique functionality needs.

Senator ROMNEY. I cannot resist asking you a personal question, which is you were in Silicon Valley. I read stories about the billionaires, the popcorn in Silicon Valley. What led you to leave Silicon Valley and go to work in the government? Are you happy you made that decision? [Laughter.]

Are you looking for a ticket back, or is this a responsibility that you particularly feel is important and that you enjoy?

Mr. HYSEN. No, sir, I am not looking for a ticket back. I have been thrilled to make this transition. I come from a family of public servants. My father is a retired public servant at the General Services Administration (GSA). When the healthcare.gov disaster occurred in 2014, was looking at the work I was doing in Silicon Valley and saw the opportunity to use my skills for a bigger purpose. I was thrilled to be able to cofound the U.S. Digital Service and have since helped recruit dozens of other technologists from the

private sector into government and look to bring on many more in the years to come.

Senator ROMNEY. I very much appreciate that, as a citizen. You described the priorities. The Chair asked about which systems you modernize. It struck me that one of those was perhaps the highest, which is protecting national security, protecting personal information that individuals might have, that there is a high degree of sensitivity there.

Are we fully modernized in that category or are we still operating some legacy systems that present a real risk, either to national security or to the personal privacy of our citizens?

Mr. HYSEN. Senator, we certainly have more work to do. Several of the systems that my colleagues here have mentioned do present cybersecurity risks through the ongoing operation of our legacy systems, and we are focused on modernizing those as rapidly as possible.

Senator ROMNEY. Let me turn now to something I mentioned in my opening statement which is AI and the impact of AI on your respective responsibilities. I am aware of the writing today and the discussion today about how vulnerable we are to machine learning to be able to break into our systems.

What is your sense of that? What are we going to need to do to protect the most critical information that we have from attack, from malign interests that would seek to undermine our national security or our personal privacy?

Mr. HYSEN. Ranking Member, thank you. As you noted, AI presents significant opportunities in modernizing our systems as well as better harnessing AI to advance our mission delivery, but the risk of adversarial use of AI is real as is the risk of disparate bias or unintended disparate impact from our use of AI.

Secretary Mayorkas recently launched a Department-wide AI Task Force that I am co-chairing, along with our Under Secretary for Science and Technology (S&T), that is looking at exactly those questions. We are still early in our work but are taking this work very seriously and have it as a major focus for the year to come.

Senator ROMNEY. Maybe it is a conjecture at this point, but any sense of what we might need to do to protect critical information from an AI attack? Do we need to almost go offline in some respects with some databases? I wonder how you can protect our systems, given the power of an AI approach.

Mr. HYSEN. Senator, one area I would start with is a little more basic than that, is even AI literacy among our employees and those with access to our data. We expect to see an increasing number of AI-generated phishing emails that are attempting to trick our employees and other users into giving up information, and we need to be able to ensure that our employees know what AI is capable of and are on the lookout as they are executing their responsibilities first.

Senator ROMNEY. Thank you.

Senator HASSAN. Thank you, Senator Romney.

I will recognize Senator Lankford for his questions.

OPENING STATEMENT OF SENATOR LANKFORD

Senator LANKFORD. Thanks for doing this hearing, and gentlemen, thanks for your testimony as we walk through this. Mr. Hysen, I want to continue the conversation with you. USCIS still uses paper for a lot of the immigration processing, so tell me the status of where we are moving right now. Obviously, there are a lot of things that are changing along the border and trying to update data systems there. USCIS seems to be lagging in some of that. Where are we?

Mr. HYSEN. Senator, thank you. I actually believe USCIS is now a success story in their digitization journey. The first project that I was assigned to work on when I joined the U.S. Digital Service was USCIS's transformation program that was seeking to digitize their nearly 7 million immigration benefits applications every year.

When we started that effort they were characteristic of the old "big bang" approach, a single vendor with proprietary technology that had been working for years and only digitized a handful of forms, and processing of those digital forms ended up being slower than paper.

We worked with USCIS to restructure the program, implement agile development, move to the cloud, and implement human-centered design practices to ensure that today a significant majority of USCIS's benefits applications are processed digitally, and they are using those capabilities to reduce their backlogs and improve their efficiency.

Senator LANKFORD. USCIS, U.S. Immigration and Customs Enforcement (ICE), and CBP, their systems do not necessarily all talk to each other in moments that they need to be able to talk to each other. Do you know of an area between the three of them, as they are trying to be more interoperable in their systems and their data links, where you do not have to actually contact somebody else to get that information? They can actually pull it as they need to.

Mr. HYSEN. Yes, Senator. Historically that has been correct, and that has been something that we have worked very hard to address over the last several years. Through our Southwest Border Technology Integration Program we have been working to digitize the processes for non-citizens encountered at the border, to include issuing Notices to Appear (NTA) digitally as well as handing off information between agencies.

One example there is ICE's new Case Acceptance System (CAS), which allows CBP to refer a case to ICE for custody digitally rather than waiting hours for ICE to come pick up a paper file and make a custody determination. This has saved millions of hours in transfer time, moving people through our process more efficiently.

Senator LANKFORD. Yes, it has been helpful. What has been interesting is there are still a couple of moments there where they still have to contact each other, and we can talk offline about some of those. I am sure your team is already making contact with you about it.

I was in Arizona, actually last week, as I am regularly down there for my responsibilities from this Committee, actually. In that dialog it was interesting to hear several folks say this system, the technology piece of it, is so much better than what it used to be, and I can see that and see the processing and the speed of that,

where you have actually got people trying to input the data and to get them out.

The challenge now is that we have more and more people that are data input folks at the border, and that is always the challenge as the human piece now. I will have a different set of questions for DHS on who should be the person actually entering all that data. Right now it is a person with a badge and a gun is also the person that is sitting there entering all the data. That is maybe not the best use of their time, to do that. But that has been a real help, but finding other ways that we can connect.

It was interesting, as well, just on a vulnerability issue, how many areas of the border where we still do not have cell coverage and are very remote. You have folks out there with a portable device trying to connect in, and obviously there is no connection. That is a larger issue to be solved. Or that when you are on the border and you get to a Border Patrol station, immediately you open your phone and it says, "Welcome to Mexico," when I am 50 feet from Mexico and you suddenly realize all the information that I am processing is processing through a cell tower on the Mexican side, not on the American side.

There are some clear vulnerabilities there. How are we handling some of those vulnerabilities with our data?

Mr. HYSEN. Senator, thank you. I have had that exact same experience during my trips down to the border. We are working to expand connectivity infrastructure along the border. It is challenging given the geography. Some of the areas we are looking at include CBP's use of mesh networking kits that can extend the coverage of their devices, as well as satellite connectivity, and in other cases looking at partnerships with other Federal agencies as well as State agencies that have land rights along the border, including in parks, that we need to look at to put up more cell towers and expand coverage. We still have work to do there, but it is something we are looking at very closely.

Senator LANKFORD. Yes, that is very helpful. Thanks for the progress on that, but we obviously still have a little bit of progress to go on it. But it is nice to see the work that is going on.

I also appreciate the off-the-shelf focus, to say if there is some technology that already exists to do this then let's invest our dollars in other areas, in other technologies, I think is where you are trying to get at as well, to say that we do not have to create this ourselves. When I am along the border, and last week, when I was there many of the agents that were there, both at the ports of entry (POEs) and between the ports of entry, their first comment was, "A lot of the folks that are coming are non-Spanish speakers." They had 1,000 people from Mauritania that came in, in the last 2 weeks, that are adult males from Mauritania that are coming in, in large numbers. Russians that are coming in, in large numbers. Pakistanis, Middle Eastern men that are coming in, that we have no criminal records for at all and have no background information. But we also have no translator that is there.

I said, "OK. How is that going?" and they all said, "Everyone shows up with their phone and with Google Translate on, and we stand there and Google Translate, communicate back and forth to each other."

I am sure there has been a push with DHS saying we need to develop our own system to be able to do this, but currently the Google Translate is working, and everyone seems to be fine with it, and it allows us to use monies in other areas that are really must-need, to develop new software technologies. In places where we can do that, we have a lot of catching up to do.

I continue to encourage you and your team to use off-the-shelf, tested software and technologies where we can, to make sure that we are investing dollars, trying to get us completely caught up with where we are not paper-based in other areas. Does that make sense?

Mr. HYSEN. Yes, sir.

Senator LANKFORD. OK. Thank you. Thanks for all the work.

Senator HASSAN. Senator Rosen.

OPENING STATEMENT OF SENATOR ROSEN

Senator ROSEN. Thank you, Chair Hassan and Ranking Member Romney. A really important hearing and I thank you all for being here today. Mr. Hysen, as a former tech person myself who now serves in government, I appreciate your work and your willingness to serve.

But I want to move right into workforce challenges because we know that they are, well, every area in our country has workforce challenges, but really particularly in legacy IT. Maintaining legacy IT systems requires a specialized workforce capable, of course, of supporting technology no longer utilized, or I would not say no longer utilized, because it is utilized, it is there, but not as nimble as we can be with newer technologies. In many cases you cannot find the skilled workers trained in dated systems. I hate to use the words "dated systems and technologies" but those kinds of things that I programmed in—Common Business Oriented Language (COBOL), FORTRAN, Assembler—from the 1980s and 1990s, you are trying to find a workforce that can maintain while you still have it, that can develop new systems, and then unload and reload, make that transition. It is really important. While we transition we have to train our IT younger generation coming up on how to do those things.

Mr. Hysen, for maintenance development, for transition design and planning, and for unloading a database and reloading it to the new system, if you will, or databases, however they are, how are you approaching this expected modernization, and what are you doing to prepare the workforce that is going to live in both of these worlds, and needs to for a little bit longer?

After that Mr. Armstrong and Mr. Oshinnaiye, if you want to talk about it as well.

Mr. HYSEN. Senator, thank you. It certainly is always an experience when I bring a new engineer or IT professional in from Silicon Valley and introduce them to how things do work in the government.

Senator ROSEN. The wonders of COBOL.

Mr. HYSEN. We are, thankfully, largely free of COBOL at DHS. I think there is probably a pocket or two there.

Senator ROSEN. The lovely Assembler, 16 bit.

Mr. HYSEN. Yes. But it certainly is a different experience than working in the private sector. We are focused on training across the board. One of the areas that I and my fellow CIOs at DHS have identified as a priority is standing up a department-wide IT academy that will include standardized training for all new IT hires into the Department as well as ongoing development opportunities for our employees to develop new skills, whether that be in AI and data science, customer experience, agile development or the like.

The IT workforce at DHS is a tremendous asset. We have over 5,000 talented and committed professionals. While we are also looking to bring in more talent from the private sector, we have opportunities and are focused on enabling our existing workforce to grow and continue to increase their impact.

Senator ROSEN. You may have to work with the private sector who is still using legacy systems in order to share data or do some of that, so it is important.

Mr. Armstrong? You laughed at my 16 bits. I appreciate that.

Mr. ARMSTRONG. I happen to be one of those legacy COBOL programmers.

Senator ROSEN. I have a hexadecimal calculator on my desk still, so there you go.

Mr. ARMSTRONG. It might have helped put my kids through college.

At FEMA—and admittedly, I have only been there about 8 months now, so I am still learning a lot about FEMA—we have a pretty aggressive program in place for retraining some of the existing staff on things like cloud technology and trying to get them, I would say, retooled for the newer technologies. But we are also in the process, unfortunately, because we have lost so many folks through attrition, of hiring a little over 100 people in IT. We are looking for newer skill sets as we are bringing people on board.

The challenge is attracting them away from industry, and you do not come into government jobs for the money, obviously. You have to really get them wanting to come in and do the mission and be part of something bigger than themselves. That is kind of our approach.

Senator ROSEN. Thank you. Mr. Oshinnaiye.

Mr. OSHINNAIYE. Thank you, Senator Rosen. What we have done at TSA, in addition to what my colleagues mentioned, is kind of reducing the fear of getting your hands dirty. Myself and my deputy are also former developers, so we allow folks to come in and use a technology. We have noticed that very new and very tenured staff, if you give them a chance to work with vendors and come in and just spend the time, they will be open to it and then use that process.

We actually had a staff member build a system themselves in the last 30 days that we are actually using internally. Once you reduce that fear factor and let everyone learn and then fail forward, we are able to build out what I call the IT IQ.

We even have, in our airports, what we call LIFT cells, innovation cells, which allow folks in the airports to come up with ideas and build on platforms. The more you let folks work and use it, the smarter they become.

Senator ROSEN. I like that IT IQ. I am going to use that one, but thank you.

I am going to move back over to you, Mr. Armstrong, and talk about FEMA disaster grants, because last month I led several of my Nevada delegation colleagues in urging the Administration to grant our Governor's request to declare a major disaster in Nevada due to severe winter storms that caused extreme flooding, rockslides, and landslides. I was pleased to see a disaster later declared, so it allows our Nevada residents, our local businesses, our Tribal communities the access to the Federal resources that they need.

But as Nevadans start to access these vital FEMA resources I want to ensure that your systems are up-to-date and secure so that my constituents can get what they need to rebuild their lives, in many cases.

Mr. Armstrong, what is the status of the FEMA Grants Management modernization, which was started in 2017, and FEMA's Individual Assistance and technical support modernization, which is really that interface that began last year?

Mr. ARMSTRONG. Sorry. The IT guy forgot to turn on his microphone.

With respect to Grants Management modernization, we have moved over 19 grant types so far. We have another 20 to move, and those are projected to be moved by April 2024. In addition to that, the program is in the process of getting a new vendor on board to start to transition data from the legacy systems into the new systems, and that is projected to start in the fall of this year.

The goal would be to get all the grants up and running by the spring of next year, data migrated over by mid-summer of next year, and decommissioning to happen sometime in 2025, of the legacy system.

Then with respect to your second question about Individual Assistance, that planning is still early on. There is some initial work that has been done to stand up a cloud environment instance as part of our bigger FEMA cloud environment. That work should be completed in the fall. Currently the program is in the planning/looking-for-funding stage to really get off the ground.

Senator ROSEN. That is our trigger, looking for funding. But I would urge putting an app as well, because most people, if they are in a disaster, what do they leave with? Just a phone. They do not maybe have the other things with them, and that is an easy way for them.

Mr. ARMSTRONG. Yes. I do not want you to get the impression that nothing is going on. There is still some work to try to help modernize some of the legacy processes that are there today. We recently, led by the Administrator, had a dogfooding session, where we brought in our executives and put them through scenarios where they get to the kick the tires on both Grants Management and Individual Assistance. We also had scenarios where we different types of survivors or different types of grant users, and had to interact with the system and give feedback to the programs. It was a good opportunity to step outside of your comfort zone and put yourself in the shoes of someone that actually has to use the system.

Senator ROSEN. Thank you. I appreciate that.

I do have one more question, Madam Chair, if there is no one waiting. Is that OK?

Senator HASSAN. Go right ahead.

Senator ROSEN. I know that Senator Romney talked about the vast amounts of data that we have and how do we keep it secure, and some of the things that are really important to us. I want to talk about the concept of Federal data centers, because in 2014, OMB launched an initiative to consolidate our Federal data centers, which has resulted in a cost savings of $5.8 billion. The Department of Homeland Security began its own data center consolidation efforts long before governmentwide Federal data consolidation efforts were launched.

DHS, you undertook this project with the objective of fostering productive collaboration and facilitating improved data sharing. In March, this Committee, we are very proud to have marked up the Federal Data Center Enhancement Act, bipartisan legislation I introduced, that requires OMB to coordinate a governmentwide effort to develop minimum requirements for Federal data centers related to cyber intrusions, data center availability, and resilience against both physical attacks and natural disasters.

Mr. Walsh, how do you assess the success of the Department of Homeland Security data center consolidation efforts?

Mr. WALSH. As you noted, data center consolidation has been a great source of cost savings in the government, and DHS, with the emphasis that they have placed on enterprise-wide services has been working toward that. A prior colleague of mine once said that if you cannot consolidate, if you cannot do it well, up to snuff, to the metrics that you are talking about, then maybe it is time for us to get out of the business. I think the government, in many cases over the past 7 or 8 years, has been doing exactly that, getting out of the business. I think DHS has been doing a good job, as you noted, toward the forefront of the government, to eliminating its data centers.

Senator ROSEN. Thank you. Thank you, Madam Chair.

Senator HASSAN. Thank you, Senator Rosen.

I have a few more questions, and then we will likely wrap up unless other Senators come on in.

Mr. Walsh, before I start with a question to you I want to note, for Mr. Hysen and all of the DHS folks here, Senator Lankford talked about the lack of cell service, for instance, on the Southern Border and the challenges that creates. It is also creating a huge challenge, as you know, on the Northern Border. I want to raise that and make sure that we are focused on trying to make sure that wherever our personnel are they have the connectivity that they need to keep us safe. I hope you will take that emphasis back with you.

Now to Mr. Walsh, Federal IT modernization projects take many years and considerable resources to plan and execute. We have been talking about that. They often face significant barriers too. For example, since 2015, DHS has been working to update its aging system that in order to assist Federal law enforcement in identifying threats integrates biometric data from across government, and I believe you commented on that in your testimony.

However, this project has run into several challenges, causing Congress to request an independent evaluation of the project.

Mr. Walsh, you mentioned that GAO has done some monitoring of DHS's progress on this particular progress. What challenges have you identified that are preventing DHS from completing this project?

Mr. WALSH. First, we are currently doing work on the Homeland Advanced Recognition Technology (HART) program, on your behalf. We are happy to chat with you at any point on the status of that work.

Our prior issued work identified a series of issues related to the HART program, and we made a total of seven recommendations. Three of those recommendations remain open. They are related to reviewing contract deliverables from contractors before accepting them, tracking and monitoring costs, defining and monitoring stakeholder involvement. Those are the three remaining recommendations—making sure that you involve your stakeholders, track your costs, and do not carte blanche accept what the contractor gives you and tells you.

However, as we have been talking, HART is one of these "big bang" approaches. It is not one of these new, smaller, fail fast, get a product out the door quick. That is a problem. I think DHS has identified their 2020 breach of this program due to overly complex and potentially high-risk design as well as disagreements with the contractors.

Senator HASSAN. Thank you.

This is a question for the three DHS representatives here. In 2020 and 2022, I wrote to DHS requesting a department-wide IT modernization plan. The Department still has not provided one. IT modernization plans play an important role in an agency's ability to make progress on their IT goals, control costs, and provide transparency.

As much as I appreciate the progress you all have reported about today I am still concerned that without an agency-wide IT modernization plan DHS will continue to struggle to prioritize updating its most critical systems.

Mr. Hysen, without a department-wide IT modernization plan, how do you ensure that the agency is meeting its goals, especially in regard to mission-critical systems?

Mr. HYSEN. Thank you. First, we are currently finalizing our updated IT strategic plan for the Department. Our current plan expires at the end of this fiscal year, and we will be releasing the new one prior to its expiration that will identify our overall modernization priorities.

But ultimately, in government, the truest sign of your priorities is where you align your budget. I have been focused, along with our acting Chief Financial Officer (CFO), on strengthening the IT oversight of our budget request. Over the last 3 years, we have progressively increased IT involvement in the annual budgeting process, under the spirit of FITARA, such that now, as we are preparing our 2025 budget request, every IT investment proposal by any part of the Department is evaluated against the IT modernization priorities that I have set out for the Department, and then we are en-

suring that my component CIOs and then ultimately I have full review and approval over the IT budget request.

Ultimately I believe that our budget request becomes the modernization plan, as that is where we intend to align our resources.

Senator HASSAN. OK. Thank you. We will follow up with you on that.

Mr. Oshinnaiye and Mr. Armstrong, how would a department-wide modernization strategy help inform TSA's or FEMA's modernization efforts? Mr. Oshinnaiye.

Mr. OSHINNAIYE. Thank you, Chair. As CIO Hysen mentioned, we actually follow in tandem with the Department on some of the components. We are also building out our strategic plan as well and working to align with the Department. Some of the things that we have adopted, in addition to technology advancement, is technology context, making sure that when we put new technology out it actually aligns to the mission. As a part of saving money on the mission is making sure we put the right technology out so people can use it, and we are not iteratively trying to change technology because it does not adapt to what the user needs.

We use that, and we work with the Department on all of our upgrades and our processes so that we are in alignment, not only to the Department but with other components. Then when we find an opportunity to share technology, we do that so we can consolidate what we are using.

Senator HASSAN. What I am hearing you say is a department-wide modernization plan will help you all align and be more efficient, more effective, get the technology you need. I am trying to understand what the benefits are.

Mr. OSHINNAIYE. Absolutely. When we are in alignment it will help us be more effective and optimal.

Senator HASSAN. OK. Mr. Armstrong.

Mr. ARMSTRONG. Thank you, Madam Chair. Traditionally, the components have been a key part of helping develop the departmental strategic plan, so I would anticipate we would be all providing input into that plan, as we all have different mission needs, different technology baselines, and so that would get incorporated into the plan.

Certainly, FEMA would benefit from having an overarching plan. We have a strategy from 2022, which will probably need to be updated in the next year, after the DHS plan is developed.

But certainly it helps, one, communicate to the non-IT leadership across the Department where are we headed, and two, it is critical, as we pointed out, about identifying mission-critical systems. It also helps identify mission-critical strategies about those systems so that throughout that budget formulation process we have a strategy to point back to, to say that this initiative is supported by this overarching strategy to help justify where we are headed, from a funding standpoint.

Senator HASSAN. Thank you.

Mr. Hysen, another question. Having adequate financial resources is obviously a key component of any IT modernization project, and in turn, smart investments in modernizing legacy IT can save taxpayer dollars. It is important that agencies have flexibility for multiyear IT modernization projects to help them navi-

gate unpredictable appropriation cycles and to keep projects running on time and on budget.

An example of this flexibility is having an IT working capital fund. DHS maintains what it calls a "non-recurring expenses fund." Can you describe the similarities and differences between that fund and a traditional IT working capital fund?

Mr. HYSEN. Thank you, Chair. Yes. Since Congress passed the Modernizing Government Technology Act, DHS had been requesting budgetary authority to establish an IT working capital fund. In the fiscal year 2022 budget, we were granted the authority to create this nonrecurring expenditures fund (NEF), that takes expired funds and allows us to spend those both on IT modernization projects but also on modernizing our facilities, which has been a critical priority for Secretary Mayorkas, to improve the experience of our employees.

We have stood that fund up. The funds there will be split 50/50 across IT and facilities. The initial investments there are on some facilities improvement projects, and we are preparing now to begin considering the first round of IT projects. We believe it does meet the intent of an IT working capital fund, even though it is technically a little different.

Senator HASSAN. It is still taking some of those resources and using them for non-IT purposes.

Mr. HYSEN. My understanding from the budget discussions, when it was being enacted, were that when we expanded the scope of the fund to facilities, we also increased the total portion of expired funds that were being transferred. Ultimately our CFO, our chief readiness support officer, and I viewed the proposal as a win-win for the Department.

Senator HASSAN. OK. But you still do not have an IT working capital fund that is devoted over years to improving the IT and modernizing IT.

Mr. HYSEN. Technically, no, but we believe that the NEF will grow considerably as funds expire, year over year, and with the intended 50/50 split with IT funding there, that that will be a long-term source of much-needed IT modernization funding for us.

Senator HASSAN. All right. Thank you.

Now to Mr. Hysen, Mr. Oshinnaiye, and Mr. Armstrong, you are all CIOs. Agency chief information officers play an important role in advocating for the IT needs of the agency. As we discussed today, you and your peers work to ensure that DHS has the technology it needs. That is obviously critical so that the agency can fulfill its mission to keep the American people safe.

Mr. Hysen, are there additional authorities that would help you do your job more effectively?

Mr. HYSEN. Chair, I believe that FITARA gave us, as CIOs, sufficient authority to effectively oversee our IT at our departments. My focus is on strengthening our internal processes to best leverage those authorities, to ensure that I am able to carry out those responsibilities fully.

Senator HASSAN. OK. Mr. Armstrong and Mr. Oshinnaiye, as the CIOs of agencies within DHS, what resources or guidance could Mr. Hysen's office provide to support your work and meet the

unique needs of FEMA and TSA? We will start with you, Mr. Armstrong.

Mr. ARMSTRONG. I have to also agree with Mr. Hysen. Having been at the Department for quite some time, I will tell you FITARA has really made a significant difference in the authorities that the CIO has. To give you an example, I come from a community where I had a lot of centralized IT under me, to an environment where IT is more spread out across the agency and more federated. However, I have a lot of checks and balances in place, and processes, so that I get to influence decisionmaking across the agency with respect to the planning of IT, the budgeting of IT, the execution piece of IT. A lot of that is through the chief acquisition executive doing regular reviews and providing oversight. But I am certainly at the table to help move that needle one way or another, where it needs to go.

I feel we have the authorities at this point in time. It is a matter of maturing them and executing them.

Senator HASSAN. Thank you. Mr. Oshinnaiye.

Mr. OSHINNAIYE. I will add, I will say FITARA has helped support my job and my role in my agency. I will say that at a Department level, CIO Hysen and staff, working with other counterparts across DHS headquarters, gives a credibility to the component to be able to have the authority to sit at a table with counterparts like the CFO or the component acquisition executive. When we want to make a change or make a mandate, if we have to, for the agency, they look to the Department, and when they see the collaboration they echo that at the component level. That has been very helpful.

Senator HASSAN. Thank you. Before we close I have asked a series of questions to the three CIOs at DHS, but Mr. Walsh, anything that you want to add or weigh in on here?

Mr. WALSH. Thank you. I would like to chime in on that last bit about CIO authorities. We took a look in GAO–22–104603 at the authorities that private sector CIOs had and compared those to our Federal CIOs, and found that, for the most part, private sector CIOs and Federal CIOs had similar authorities.

However, we did make a pair of recommendations, one of which was to OMB to enhance the coordination not between CIOs but between the other C-suite executives, so making sure that the C-suite plays nice together. I do think that is relevant here. The CIOs perhaps have the authority. Now getting the C-suite all on the same page is the next challenge.

Senator HASSAN. I appreciate that very much because that has been my experience too. Even when the authorities may be in place, making sure that everybody is actually recognizing that they exist, and including your voices in the planning and budgeting process and prioritizing work in the agency is really important.

I will also just note that if there are authorities that you realize you need and do not have, or ambiguity about your authority creates barriers, we need to know about that because that is obviously something we can work with you to address. But if you all do not speak up and let us know, we cannot help you with that.

I want to thank all of you—Mr. Hysen, Mr. Oshinnaiye, and Mr. Armstrong—for your testimony today, and to the three of you for

the important work that you do for the Department of Homeland Security. The first job of government is to keep people safe, and I am very grateful that you are working to do that, along with your colleagues each and every day. Thank you, Mr. Walsh, to you and your colleagues at the Government Accountability Office, for providing accountability and guidance to make DHS's work more successful.

The hearing record will remain open for 15 days, until 5 p.m. on June 15th, for submissions of statements and questions for the record, and this hearing is now adjourned.

[Whereupon, at 11:26 a.m., the hearing was adjourned.]

APPENDIX

Opening Statement as Prepared for Delivery by Chair Maggie Hassan
Emerging Threats and Spending Oversight Subcommittee Hearing:
"Securing the Nation: Modernizing DHS's Mission-Critical Legacy IT Systems"
May 31, 2023

Good morning, and welcome to our distinguished panel of witnesses. Thank you for appearing today to discuss the Department of Homeland Security's reliance on aging information technology systems as it works to secure the nation, and why it is crucial that the Department and its component agencies modernize their mission-critical systems.

I also want to thank Ranking Member Romney and his staff for working with us on this hearing, and for our continued partnership to address emerging threats and reduce wasteful government spending.

Today's hearing continues our subcommittee's work to replace aging government technology that wastes taxpayer dollars, undermines our security, and limits government's efficiency and responsiveness. As our subcommittee continues to encourage agencies to adopt modern systems that are more efficient, more cost-effective, and, frequently, more capable, we will hear today from senior DHS officials about how outdated technology negatively impacts the Department's budget and our nation's safety. For example, if an aging system that DHS uses to vet passengers or visitors traveling into or through the United States goes offline, there's a chance that a dangerous person could enter the country. In such cases, work-arounds can help limit national security risks, but they can also cause commercial delays or miss real-time intelligence.

The Government Accountability Office and the DHS Inspector General have assessed DHS's IT modernization efforts and raised concerns about its reliance on outdated IT systems to perform mission-critical operations. They have looked at DHS IT systems that ensure the security of air travel, support disaster mitigation and preparedness activities, and enhance border security, and they have asserted that the failure of any of these systems would have a significant impact on public safety and national security. That is why it is crucial that DHS modernize these systems.

Today's hearing is an opportunity to examine how legacy information technology is a threat to national security and how DHS can responsibly update its systems. I look forward to hearing from all of our witnesses about the risks posed by legacy IT systems at DHS, and how DHS can successfully modernize these systems to keep the American people safe, secure, and free.

Opening Statement
Ranking Member Mitt Romney
U.S. SENATE SUBCOMMITTEE ON
EMERGING THREATS AND SPENDING OVERSIGHT
"SECURING THE NATION: MODERNIZING DHS'S MISSION-CRITICAL LEGACY IT SYSTEMS."
MAY 31, 2023

Thank you, Chair Hassan, for holding this hearing. I appreciate the witnesses being here to discuss how we can improve DHS's IT modernization efforts. This effort is critical to national security, as bad actors and adversaries constantly seek to access our government systems. Just last week, it was reported that a Chinese state-sponsored group known as "Volt Typhoon" targeted U.S. critical infrastructure sectors. I'm interested to hear from our witnesses about how the modernization of IT systems could help mitigate vulnerabilities to cyber-attacks across Federal networks. We cannot afford to continue operating systems that are unable to keep up with the evolving threats we face.

While meaningful steps have been taken in recent years, there is more work to do, especially as emerging technologies like artificial intelligence can be weaponized in cyber-attacks by our adversaries. We cannot continue to sit back and play defense while China and Russia ramp up these attacks.

Our government must also work to responsibly modernize IT systems to save taxpayer money. According to GAO, the U.S. government spends more than $100 billion each year on the operation and maintenance of its IT systems. If we spend that much money on IT, the systems need to work. If they don't, we need to quickly replace them.

I'm interested to learn why it is such a challenge for the government to upgrade its IT in comparison to the private sector, particularly when the data held by government agencies is so sensitive. Why isn't this happening faster?

Thank you, Madam Chair.

TESTIMONY OF

Eric Hysen
Chief Information Officer
U.S. Department of Homeland Security

Charles Armstrong
Chief Information Officer
Federal Emergency Management Agency

Opeyemi Oshinnaiye
Assistant Administrator for Information Technology
Transportation Security Administration

BEFORE

Committee on Homeland Security and Governmental Affairs
Subcommittee on Emerging Threats and Spending Oversight
United States Senate

ON

"Securing the Nation: Modernizing DHS's Mission-Critical Legacy IT Systems"

May 31, 2023
Washington, DC

Chair Hassan, Ranking Member Romney, and distinguished Members of the Subcommittee, on behalf of my colleagues from the Transportation Security Administration (TSA) and the Federal Emergency Management Agency (FEMA), we thank you for the opportunity to testify at today's hearing, "Securing the Nation: Modernizing DHS's Mission-Critical Legacy IT Systems."

We are focused on modernizing legacy IT systems for a host of important reasons, notably strengthening information security, assisting in eliminating unnecessary spending, and better leveraging data as a strategic asset. Most importantly, we modernize to deliver critical mission capabilities and improve the services government delivers to the American people more effectively.

My colleagues and I here today and across the Department of Homeland Security (DHS or Department), work as a team to help modernize the vast array of critical missions undertaken by DHS—everything from facilitating international trade to responding to disasters to improving federal government information security practices. Our collective successes and lessons learned inform our distinctive take on IT modernization. While there is always work to do, we have made progress and appreciate the opportunity to share it with you today.

The Department's Approach

Historically, agencies across the federal government, including DHS, took a "big bang" approach toward IT modernization. At its most basic level, the Department attempted to acquire and deploy IT systems in the same way we acquire and deploy ships. Government staff spent years gathering requirements, awarding a large contract to a single systems integrator to build to exact requirements and test extensively against them. In theory, the new, modernized system would launch, the legacy system would be decommissioned, and the new system would go into ongoing maintenance for years until it was time to modernize it again.

In practice, however, this approach—known as "waterfall" software development—typically leads to modernization programs going over budget and behind schedule at high rates. Requirements gathered over years in large scale plans are often out of date well before a system is deployed. Over reliance on a single large system integrator means federal staff sometimes lack necessary skills and access to lead technical programs, make required inherently governmental technical decisions in the interest of the government and the American people, and address inevitable problems that arise with large complex programs. The single "big bang" release of a new system leads to massively increased risk, as the nation saw loud and clear with Healthcare.gov.

At DHS today, we reject this approach in favor of a more incremental, iterative, and measured strategy based on private sector best practices that enable us to successfully modernize key services and retire costly legacy systems. Our newly-initiated modernization programs focus on defining a Minimum Viable Product—initial functionality that can launch within months, not years. From there, the Department follows an agile software development methodology that gathers requirements, builds, tests, and launches software in rapid, iterative cycles rather than waiting to gather all requirements up front. Modernized systems are implemented in parallel to legacy systems to buy down risk over time. For existing programs started under the old model,

DHS focuses on transitioning as much work to the new method as possible. This overall approach breaks down into two strategies—a technical approach to IT modernization and cultivating tools and resourcing to get the job done.

I. Technical Approach to Legacy Modernization

At DHS, we build upon existing infrastructure based on a few key principles. First among these principles, the Department, not a contractor, should serve as lead integrator for any modernization effort. We still rely on our industry partners for critical expertise and services while ensuring we have strong federal staff with technical and subject matter expertise to maintain control of modernization programs throughout their lifecycles and ensure the work of contractors and internal teams comes together to deliver results.

We implement modern software development practices throughout the Department. Agile project management allows us to break down large programs into smaller sprints and launch functionality, iteratively over time. In line with the Administration's focus on customer experience, we work to ensure experts in human centered design conduct up front user research to inform requirements and extensively test prototypes for suitability with potential users throughout the process. DHS leverages continuous integration, continuous delivery tools, and modern cloud infrastructure to deploy new functionality every few hours or days, rather than waiting months.

Beyond our integration role and embrace of modern software development, our technical approach also leverages enterprise services for use across the Department and across the interagency. In the past, issuing a single large contract to a system integrator for an entire IT program often meant that integrator would build every part of the program from scratch, leading to a proliferation of duplicative infrastructure, software components, and support services such as help desks, login systems, and development toolkits. This increases cost, slows down development as each program seeks to repeat the same tasks, and increases cybersecurity risk by offering more targets for our adversaries.

To address these challenges, the Department is driving adoption of reusable enterprise services across IT programs, allowing our development teams to focus on the mission that their efforts will serve. For example, we offer enterprise cloud services to avoid redundancies among our Components, centralize expertise and operations, and ensure maximum reliability. We also created a system across the Department equipping developers with access to common tools, tracking features for tasks within the development life cycle, and a repository for source code so our professionals can see and leverage the work of others while saving money. Authentication is another area where we envision gains in both savings and security through development of secure, shared internal identity platforms and adoption of external shared services including the General Services Administration's (GSA) Login.gov. Finally, we adopted initiatives like the Network Operations Security Center, which combined five headquarters Security Operations Centers and four Network Operations Centers into one DHS enterprise service to create savings and enhance reliability for the Department's cybersecurity operations.

II. Tools & Resourcing – People, Funding, Contracts

This new technical approach to legacy modernization requires an equally significant shift in approach to personnel, funding, contracting, and governance to achieve success. We must attract, hire, grow, and retain top technical talent across the Department and at the operational Components. In 2021, the Department launched the DHS Cybersecurity Talent Management System, an entirely new personnel system that provides flexibilities in recruiting, assessing, compensating, and developing technologists. Over 100 employees have onboarded under the new system thus far within the DHS Office of the Chief Information Officer (CIO) and the Cybersecurity and Infrastructure Security Agency (CISA), and we are actively expanding the program to FEMA later this year. Additionally, in 2022, we partnered with the U.S. Digital Service (USDS) and Office of Personnel Management to launch the federal government's largest-ever hiring initiative for customer experience professionals, bringing 25 new employees into DHS and offering up additional qualified candidates for hiring across the government.

We are also building new programs to better train our IT professionals across DHS. These include a planned DHS IT Academy, which will create standard technical orientations for all DHS IT employees, develop a rigorous training and rotation program for entry-level hires, and offer upskilling opportunities for employees to learn new and emerging skills in areas including data science, artificial intelligence, and human-centered design.

DHS also continues to rely heavily on expertise from across the federal government. USDS supported U.S. Citizenship and Immigration Services (USCIS) and U.S. Customs and Border Protection (CBP) in transforming key programs and leading the Department in their modernization journeys. Additionally, GSA's Technology Transformation Services and 18F played critical roles in early modernization efforts at TSA and USCIS.

In addition to new tools to hire and develop our people, DHS needs new models to fund IT modernization. We were one of the first users of the Technology Modernization Fund (TMF), in 2020 securing $15 million in funding to complete a critical portion of modernizing CBP's Automated Commercial Environment trade system. We also recently received $50 million in TMF funding for the Southwest Border Technology Integration Program and $26.9 million for modernizing the Homeland Security Information Network (HSIN). Through these experiences, we learned that the TMF is a critical tool for certain types of modernization projects, but not the right fit in every situation. When TMF is not the best funding tool, DHS appreciates Congressional authorization through the previous year's appropriations bill to target IT modernization and facilities with our new Nonrecurring Expenditure Fund (NEF), which honors the intent of the Modernizing Government Technology Act. The NEF offers a valuable new funding mechanism for modernization projects which directly improve customer and employee experience or strengthen cybersecurity, under the oversight of the DHS CIO and DHS CIO Council.

The Department will use these new funding approaches with existing authorities under the Federal IT Acquisition and Reform Act (FITARA) to bring modernization into alignment with IT budgeting. To facilitate alignment, the Department developed new tools such as the Unified Cyber Maturity Model (UCMM)—which qualitatively assesses cybersecurity—to focus and

assess risk reviews. For modernization programs, assessments under UCMM are critical to determine future investments. At the contractual level, use of the Department's acquisition review process under FITARA also provides oversight to ensure our new "modernize in place" approach succeeds for newly initiated programs even while DHS transitions legacy waterfall efforts to modern iterative practices.

Progress and Challenges at DHS Headquarters

When DHS was founded, IT at our headquarters offices (including the Management Directorate, Office of the Secretary and Executive Management, and other offices without a named CIO) was mostly limited to networking and infrastructure, end user services, and IT governance and planning, without many mission IT systems. As the Department matured over the past 20 years, more significant IT systems are now under direct purview of the DHS Headquarters (HQ), requiring a shift in CIO engagement with HQ offices to support effective modernization.

Our enterprise Platform as a Service offerings were critical to enabling rapid development of tools to respond to emerging mission needs without creating bespoke IT programs in each instance. We have used these capabilities to quickly launch systems in support of a variety of DHS missions.

DHS HQ also has several "big bang" IT modernization efforts which have been underway for many years. Over the past two years, however, we have focused on increasing DHS CIO engagement in these programs and transitioning them to more iterative, nimble approaches.

I. Homeland Advanced Recognition Technology

The Office of Biometric Identity Management, within the Management Directorate, has worked for years to replace IDENT, the Department's legacy centralized biometric information system, with the modernized Homeland Advanced Recognition Technology (HART) system. IDENT is one of the Department's most critical legacy systems, providing biometric enrollment and matching services to 45 DHS, interagency, and international partners with approximately 365,000 searches per day. Outages or issues with IDENT can have devastating impacts for travel, border security, and other critical law enforcement missions across the nation.

The HART program followed nearly every tenet of the old, "big bang" modernization approach and has faced significant challenges and delays. These delays were due to a combination of poor requirements definition and a lack of agility in both technical and IT acquisition approaches. Earlier this year, the DHS Acquisition Review Board conducted an extensive technical and programmatic review of HART, and the Acting Under Secretary for Management approved a more iterative plan to implement an architecture refresh and structural changes to better enable HART to reach initial operating capability in the next two years.

II. Financial Systems Modernization

In 2017, DHS established the Financial Systems Modernization (FSM) initiative managed by the Office of the Chief Financial Officer (OCFO) within the Management Directorate to transition antiquated United States Coast Guard (USCG), FEMA, and U.S. Immigration Customs Enforcement (ICE) financial systems and processes to three modern, integrated solutions to improve the accuracy and timeliness of financial information. These systems use outdated technology that is incredibly expensive to maintain, have limited integration ability, and do not support DHS standards of enhanced efficiency and security.

In December 2021, a rollout of FSM to the USCG caused appreciable system performance issues and outages. To address the significant issues raised for the initiative by this rollout, OCIO began to work with OCFO in earnest to transition this program away from "big bang" thinking and toward more agile methodologies. Through technical recommendations and improvements, reorientation of the project to ensure that government has enough oversight of the integration function, and iterative development through rolling phases bringing FSM online for new DHS Components, we plan to make improvements and contract awards by the end of Fiscal Year (FY) 2023.

III. Homeland Security Information Network

Both HART and FSM are under transitions from "big bang" to incremental modernization approaches. In contrast, in 2021, DHS launched a modernization effort for HSIN following incremental best practices from the beginning. HSIN is an operational information sharing platform relied on by federal, state, local, tribal, and other partners for receiving critical intelligence from DHS both daily and during national events from hurricanes to Super Bowls. The system is currently built on outdated technology and no longer effectively meets evolving operator needs. Based on user feedback, in 2022, the Department designed and launched a new DHS Intel mobile app to allow partners to access intelligence products on their smartphones. Rather than waiting for a fully modernized HSIN system, the new mobile app uses existing system funds. This launch helped support our successful application for TMF funding and is now the cornerstone of our broader efforts to modernize the full HSIN system iteratively over the next several years.

In summary, despite the challenges of transitioning to modern approaches for older programs, the Department's trajectory is clear – agile technology bolstered by talent creativity on funding and a bias against wheel reinvention are quickly becoming the norm at HQ.

Progress and Challenges at FEMA

Like the Department overall, FEMA's IT modernization program is designed to enhance the Agency's response, recovery, and resilience posture by making FEMA's IT more nimble, agile, user friendly, transparent, accessible, secure, and cost effective, while increasing the speed of program service delivery, reducing system redundancy, and utilizing state of the art technology.

I. Grants Management Modernization (GMM)

FEMA is consolidating eight disparate legacy systems into the FEMA Grants Outcomes System, better known as FEMA GO, for disaster and non-disaster grants. This suite of legacy systems covers the following services areas: user communities' interface for grants management; public assistance and mitigation applications and grant management; non-disaster grant management; grant reporting for state, local, tribal, and territorial governments, and non-profits; and records management for environmental and historic preservation data collection.

Migration of legacy data and decommissioning of legacy systems is scheduled for completion in FY2024-2025. We are employing a phased data migration approach to mitigate delays and ensure data migration begins on schedule in the fourth quarter of FY2023.

As a result, GMM, through FEMA GO, supported five grant programs in FY2018-2022 and onboarded 14 additional grant programs for FY2023 funding opportunities. From May 2023 to April 2024, FEMA looks to onboard 20 additional grant programs, including the security grants portfolio and disaster grants—namely, Hazard Mitigation, Fire Management Assistance, and Disaster Case Management.

Grants serve as the primary mechanism FEMA uses to accomplish its mission. FEMA currently manages over 40 active grant programs distributing well over $25 billion to state, local, tribal, and territorial governments and certain non-profit organizations to help communities respond to, recover from, mitigate losses created by, and increase resilience against disasters and other threats. A failure of the GMM program or the FEMA GO system would create additional burden and challenges for these communities, and especially for disadvantaged and isolated communities, to take advantage of FEMA grant programs and these federal investments.

II. National Flood Insurance Program (NFIP) Pivot System

Congress established the NFIP to encourage communities to make wise land use decisions and, in return for the community enacting floodplain management ordinances consistent with federal standards, the NFIP makes available flood insurance that allows people to protect homes and commercial property in flood-prone areas.

Pivot was an agile modernization project in the newer model of technology modernization replacing the NFIP IT System and Services program. Pivot processes millions of transactions for flood insurance and claims in real time, provides business workflows to automate manual processes, and provides reporting and data analytics for financial and business requirements. Pivot met Full Operational Capability (FOC) on October 1, 2020, ahead of schedule and under budget. Pivot migrated to the FEMA Enterprise Cloud on January 23 of this year. NFIP is a strong example of continuous modernization. Even after the program reached FOC, it continues to deliver new technical and business functionality to meet evolving mission needs, making it less likely to be replaced by another large modernization program.

Pivot tracks 4.7 million insurance policies with over $1.2 trillion dollars in coverage and supports the insurance companies' ability to sell flood insurance policies and pay claims during

disasters. Modernizing NFIP's systems has allowed FEMA to better support Americans at times when they face their greatest need.

III. Individual Assistance Technical Support Services (IATSS) Program

FEMA looks to consolidate multiple disparate systems into the Individual Recovery Information System (IRIS) over the next several years, with a targeted completion of July 2027.

To better support customers, IRIS will absorb multiple service areas: Individual Assistance (IA) registration; inspections and eligibility determinations; approved payment data for states; vendor mail utility for registrants; and temporary housing management. FEMA requested funding for further modernization for IA Mass Care and Automated Construction Estimator (ACE) systems. Resources are programmed in the Future Years Homeland Security Program (FYHSP) beginning in FY2025. Until then, existing budgets cover current efforts.

FEMA's IA program helps to meet the basic needs of disaster survivors and supplement disaster recovery efforts. Interfacing with the public in a clear manner supported by the latest technology qualifies as a basic tenet of success for this mission.

IV. Continuous Modernization of Network and Cloud Infrastructure

Beginning in 2019, FEMA engaged in the continuous modernization of the network infrastructure. FEMA Enterprise Network (FEN) modernization is the product of infrastructure recapitalization spanning the past five years. The FEN is the foundational data transmission infrastructure comprised of network devices and supporting services, which enable user and services data transmission enterprise wide.

Unlike the "big bang" approach, in 2022, data center migration to the cloud began to avoid recapitalization of legacy hardware. Hardware failures present continuity of operations risks, and end of life supportability creates service delivery risks and cyber security risks. FEMA anticipates finalizing the full cloud migration by the end of FY2024.

In summary, FEMA like the Department as a whole is opting for a new approach expressing more modern technologies over old waterfall systems. This includes transitions of older systems and the challenges that entails.

Progress and Challenges at TSA

TSA's modernization strategy reflects the overall DHS approach by leveraging adaptive maintenance to sustain modernized platforms. In addition, the DHS approach appears in TSA tactics such as identifying priority features for delivery and iteratively deploying and maximizing human centered design with rapid customer feedback. This enables the right features to deploy to the right users. Taking advantage of cloud platforms to get greater scale and return on investment enables TSA to outsource modernization to the platform and sustain these features inherently.

Continuing to use modern patterns, such as executing agile development and ensuring we provide top notch customer experience while building systems rapidly, allow TSA to sustain modernization and deliver quality systems.

I. Mission Scheduling and Notification System (MSNS)

MSNS is an aggregate of nine system components that enable deployment of Federal Air Marshals on flights in accordance with risk-based prioritization to protect U.S. air carriers, airports, passengers, and crews. Product improvement continued in response to operational requirements since MSNS started operations in July 2002. The system is currently undergoing modernization via adaptive maintenance to address inadequacies of in end-of-life architecture that was primarily designed for the airline industry and is not efficient in addressing the dynamic operational requirements of the FAMs. The objective of adaptive maintenance is to expedite delivery of critical capability needs within MSNS using a phased prototype driven approach that takes into account enterprise-wide infrastructure and resource reuse.

Adaptive maintenance of MSNS includes design, development, and deployment of solution components on to a cloud that incorporates native services, human-centric design, mobile enabled, data driven, and enhanced security. This will result in significant cost savings by sunsetting legacy system components and associated operations and maintenance services. This approach will help deliver a fully modernized MSNS by the end of FY2025.

II. Performance and Results Information System (PARIS)

PARIS is the system of record for TSA's Security Operations regulatory compliance data. It maintains information associated with TSA's regulatory investigations, security incidents, and enforcement actions and records details of security incidents involving passenger and property screening. TSA relies upon this system to provide the highest traveling public security standards.

In fourth quarter of FY2019, as part of adaptive maintenance initiative, legacy PARIS was re-architected to migrate to a Software as a Service (SaaS) government cloud. The newer PARIS became operational in second quarter of FY2021 and access to all historic compliance data was completed in second quarter of FY2023. PARIS migration propelled the inspection workforce off an 18-year-old on premise custom developed application with high operational cost to the TSA enterprise SaaS cloud platform. A US Government Accountability Office audit performed in 2022, identified the following PARIS improvements: user experience; data visibility; data stewardship; and customer engagement. These were addressed successfully via multiple initiatives including workflow automation, streamlines records management, complete visibility to historic data, stakeholder advisory board establishment, among other things.

III. Staffing Scheduling Time and Attendance (SSTA)

SSTA is an enterprise-level capability for airport personnel that integrates multiple TSA systems required for forecasting, staffing, scheduling, and tracking time and attendance. SSTA streamlines airport functions with a centralized platform and workflows to address scheduling requirements and provides Transportation Security Officers (TSOs) with self-service capabilities including leave and shift trade requests. It reduces the administrative burden on airports based on

current manual/paper-based processes and decreases resource requirements, allowing officers to return to more operational roles. It also improves airport scheduling operations with near real-time data to determine resource needs and optimization.

TSA's SSTA program includes Scheduling Management and Resource Tasking; Electronic Time, Attendance, and Scheduling; and Enhanced Staffing Model. Among other accomplishments, SSTA enabled a shift to automated, remote bidding for TSO work shifts and annual leave during COVID-19, eliminating the need for in-person bidding at the airports.

IV. Secure Flight

Secure Flight (SF) strengthens security of commercial air travel into, out of, over, and within the United States and for travel between two foreign locations on a U.S. carrier. The program addresses the need for security against potential threats for flights by delivering efficient, effective security prescreening of individuals attempting to travel by air. The SF system identifies high- and low-risk passengers to mitigate known and unknown threats to aviation security and designate them for enhanced screening, expedited screening, or prohibition from boarding a covered flight, as appropriate. The SF system is highly available and geographically dispersed, processing messages from airlines and returning a Boarding Pass Printing Result within four seconds. SF is in the operations and support lifecycle phase. The SF program uses agile methodologies and replaced manual testing with a fully automated testing suite early in lifecycle development.

The program continues to maintain a high availability posture for SF while establishing a cloud migration roadmap. Cloud migration reduces the cost of maintaining proprietary hardware and software. As one of the key anti-terrorism programs supporting the larger homeland security mission, SF requires cloud migration to help to prevent mission risks through greater reliability to ensure continued safety and security of our traveling public.

Conclusion

Challenges of modernizing legacy IT are as complex as the missions that the Department and its operational Components serve. While older "big bang" modernization efforts still require close attention, the Department is turning a corner toward a more contemporary approach of modernizing in place. The stakes for expediting this transition could not be higher.

DHS interacts more frequently each day with the American public than any other federal agency, from travelers moving through air, land, and seaports of entry, to businesses importing goods into the country, to disaster survivors applying for assistance, and noncitizens applying for immigration benefits. The DHS IT community is committed to delivering modernized, secure, effective, and usable systems to support these missions. We take that responsibility seriously and look forward to working with Congress to make sure our technology modernization efforts match our ambitions.

Thank you again for the opportunity to testify today and we look forward to your questions.

United States Government Accountability Office

Testimony

Before the Subcommittee on Emerging Threats and Spending Oversight, Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. ET
Wednesday, May 31, 2023

INFORMATION TECHNOLOGY

DHS Needs to Continue Addressing Critical Legacy Systems

Statement of Kevin Walsh, Director, Information Technology and Cybersecurity

GAO-23-106853

GAO Highlights

Highlights of GAO-23-106853, a testimony before the Subcommittee on Emerging Threats and Spending Oversight, Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

Each year, the federal government spends more than $100 billion on IT and cyber-related investments. Of this amount, agencies have typically reported spending about 80 percent on operations and maintenance of existing IT, including legacy systems. DHS's expected IT spending for fiscal year 2023 is about $10.1 billion; operations and maintenance is expected to consume about $8.8 billion of that total.

Maintaining legacy systems (i.e., systems that are outdated or obsolete) can pose significant challenges. GAO reported in 2016 that agencies had system components that were at least 50 years old and vendors that were no longer providing support for hardware or software. In 2019, GAO reported that several critical federal legacy systems used outdated languages, had unsupported hardware and software, and were operating with known security vulnerabilities.

GAO was asked to testify on its past legacy system reports and DHS's efforts to modernize. Specifically, GAO summarized (1) DHS's critical legacy IT systems and plan for modernizing, and (2) progress and challenges with selected DHS IT modernizations. This statement is based on issued GAO reports and updated information on the department's implementation of GAO's recommendations.

What GAO Recommends

In a 2019 report, GAO recommended to DHS that it develop a modernization plan for its most critical legacy system. The department implemented this recommendation in February 2022 and has implemented several GAO recommendations on modernizing other legacy systems.

View GAO-23-106853. For more information, contact Kevin Walsh at (202) 512-6151 or walshk@gao.gov.

May 31, 2023

INFORMATION TECHNOLOGY

DHS Needs to Continue Addressing Critical Legacy Systems

What GAO Found

GAO reported in June 2019 that, of the 65 critical legacy IT systems identified by federal agencies as needing modernization, the Department of Homeland Security (DHS) had three such systems (see table). Further, GAO identified DHS's System 4 as one of the 10 most critical legacy systems across the federal government in need of modernization.

Table: Critical Legacy Systems in Need of Modernization According to DHS, as of June 2019

System name[a]	Age of system, in years	Age of oldest hardware, in years	System criticality (according to DHS)	Security risk (according to DHS)
System 4	8-11	11	High	High
System L	9	2	High	Moderately low
System M	6	1	High	Low

Source: GAO analysis of Department of Homeland Security (DHS) data. | GAO-23-106853

[a]Due to sensitivity concerns, GAO substituted alphanumeric identifiers for the names of the agencies' systems. GAO assigned a number to identify each of the 10 most critical legacy systems in need of modernization and assigned a letter to identify the remaining 55 systems. The identifiers in the table reflect how DHS's system names appeared in the 2019 report (GAO-19-471).

In evaluating agencies' modernization plans for the 10 most critical legacy systems, GAO determined that DHS lacked a complete plan for modernizing System 4. Specifically, DHS's plan did not include milestones to complete the modernization and did not describe the planned disposition of the existing legacy system. In February 2022, the department implemented GAO's recommendation by updating its modernization plan to include milestones for replacing the system and removing legacy hardware. By documenting its plan in sufficient detail, DHS increased the likelihood that the modernization will succeed.

GAO has also previously reported on DHS's efforts to modernize and replace other legacy systems that support financial management, biometric identity management, and grants management. Specifically,

- In February 2023, we reported that, after attempting to modernize its financial management systems for decades, DHS implemented a governance structure to oversee component-level financial systems modernizations. However, the Coast Guard was unable to declare full operational capability as expected because it had not remediated issues from operational testing.
- In June 2021, we reported that DHS's Homeland Advanced Recognition Technology program (intended to replace an outdated system for biometric identity management) was significantly behind schedule and had exceeded its estimated costs. We also found that DHS had not fully addressed key risk management and IT acquisition practices.
- In April 2019, we reported that the Federal Emergency Management Agency's Grants Management Modernization program (intended to replace 10 legacy systems) had not fully addressed leading practices for business process reengineering, requirements, and cybersecurity risk management. The program also did not meet leading practices for a reliable schedule.

DHS has now implemented 11 of the 19 recommendations GAO made in these reports. Implementing the remaining eight will help the department ensure these critical legacy systems are successfully replaced.

Chair Hassan, Ranking Member Romney, and Members of the Subcommittee:

I am pleased to participate in today's hearing on the Department of Homeland Security's (DHS) legacy IT systems. Each year, the federal government spends more than $100 billion on IT and cyber-related investments. Of this amount, agencies have typically reported spending about 80 percent on the operations and maintenance of existing IT investments, including legacy systems.[1] DHS's expected IT spending for fiscal year 2023 is about $10.1 billion; operations and maintenance is expected to consume about $8.8 billion of that total.

Maintaining federal legacy systems can pose significant challenges. For example, in May 2016, we reported instances where agencies had systems with components that were at least 50 years old and had vendors that were no longer providing support for hardware or software.[2] Likewise, in June 2019, we reported that several of the federal government's most critical legacy systems used outdated programming languages, had unsupported hardware and software, and were operating with known security vulnerabilities.[3]

As you requested, my testimony today discusses DHS's efforts to modernize its legacy IT systems. Specifically, it summarizes (1) DHS's critical legacy IT systems and plan for modernizing and (2) progress and challenges with selected DHS IT modernizations. This statement is based on issued GAO reports and updated information on the status of the department's implementation of GAO recommendations. Detailed information on the objectives, scope, and methodology for the issued reports can be found in the reports cited in this statement.

We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions

[1]The provisions commonly referred to as the Modernizing Government Technology (MGT) Act define a legacy IT system as a system that is outdated or obsolete. National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, Div. A, Title X, Subtitle G, § 1076(8), 131 Stat. 1586, 1587 (2017).

[2]GAO, *Information Technology: Federal Agencies Need to Address Aging Legacy Systems,* GAO-16-468 (Washington, D.C.: May 25, 2016).

[3]GAO, *Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems,* GAO-19-471 (Washington, D.C.: June 11, 2019).

based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Historically, the federal government has had difficulties acquiring, developing, and managing IT investments. As a result of these difficulties, we identified "Improving the Management of IT Acquisitions and Operations" as a high-risk area in 2015.[4] We designated DHS's management functions as high risk in 2003, and most recently narrowed the high risk area to "Strengthening DHS IT and Financial Management Functions" in 2023. Further, federal agencies have struggled with appropriately planning and budgeting for modernizing legacy systems, upgrading underlying infrastructure, and investing in high quality, lower cost service delivery technology. The consequences of not updating legacy systems has contributed to, among other things, security risks, unmet mission needs, staffing issues, and increased costs.

- **Security risks**. Legacy systems may operate with known security vulnerabilities that are either technically difficult or prohibitively expensive to address. In some cases, vendors no longer provide support for hardware or software, creating security vulnerabilities and additional costs. For example, in October 2017, the Office of Personnel Management's (OPM) Office of the Inspector General reported that the agency's IT environment contained many instances of unsupported software and hardware, where the vendor no longer provided patches, security fixes, or updates for the software.[5] The report noted that as a result, there was increased risk that OPM's IT environment contained known vulnerabilities that would never be

[4]GAO's high-risk program identifies government operations with vulnerabilities to fraud, waste, abuse, and mismanagement, or in need of transformation to address economy, efficiency, or effectiveness challenges. Every two years, we issue an update that describes the status of these high-risk areas and actions that are still needed to assure further progress and identifies new high-risk areas needing attention by Congress and the executive branch. We continue to identify this area as high risk. GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas,* GAO-23-106203 (Washington, D.C.: Apr. 20, 2023).

[5]U.S. Office of Personnel Management, Office of the Inspector General, *Final Audit Report: Federal Information Security Modernization Act Audit Fiscal Year 2017*, Report Number 4A-CI-00-17-020 (Washington, D.C.: Oct. 27, 2017).

patched and could have been exploited to allow unauthorized access to data.

Additionally in November 2017, the Department of Education's Inspector General identified security weaknesses that included the department's use of unsupported operating systems, databases, and applications.[6] By using unsupported software, the department put its sensitive information at risk, including the personal records and financial information of millions of federal student aid applicants.[7]

Further, in January 2023, we reported that about 33 percent of the Internal Revenue Service's (IRS) applications, 23 percent of the software instances in use, and 8 percent of hardware assets were considered legacy.[8] This included applications ranging from 25 to 64 years in age, as well as software up to 15 versions behind the current version. The IRS acknowledged that operating in this environment would continue to contribute to security risks, among other challenges.

- **Unmet mission needs**. Legacy systems may not be able to reliably meet mission needs because they are outdated or obsolete. For instance, in 2016, the Department of State's Inspector General reported on the unreliability of the Bureau of Consular Affairs' legacy systems.[9] Specifically, during the summers of 2014 and 2015, outages in the legacy systems slowed and, at times, stopped the processing of routine consular services such as visa processing. For example, in June 2015, system outages caused by a hardware failure halted visa processing for 13 days, creating a backlog of 650,000 visas.

  Additionally, in January 2023, we reported that the IRS' 60-year old system for individual tax data, the Individual Master File (IMF), needed to be modernized to help address business and technical

[6]Department of Education, Office of Inspector General, *FY 2018 Management Challenges*, (Washington, D.C.: November 2017).

[7]According to Education's Office of General Counsel, Education has developed corrective action plans to address the Inspector General's recommendation.

[8]GAO, *Information Technology: IRS Needs to Complete Modernization Plans and Fully Address Cloud Computing Requirements,* GAO-23-104719 (Washington, D.C.: Jan. 12, 2023).

[9]U.S. Department of State, Office of Inspector General, *Inspection of the Bureau of Consular Affairs, Office of Consular Systems and Technology*, ISP-I-17-04, (Arlington, VA: December 2016).

challenges. Such challenges included the inability to get a real-time view of the taxpayer's account and provide additional information to combat fraud and identity theft. We reported that the IRS had suspended the operations of six initiatives, including two that are essential to replacing the IMF. According to officials, the suspensions were due to IRS's determination to shift resources to higher priorities, and staff members working on these suspended initiatives were reassigned to other projects. As a result, the schedule for these initiatives was undetermined, and the 2030 target completion date for replacing the IMF became unknown. We reported that this would lead to mounting challenges in continuing to rely on a critical system with software written in an archaic language requiring specialized skills. IRS officials subsequently reported in April 2023 that they now plan to use additional funding to complete IMF system modernization by fiscal year 2028.

- **Staffing issues.** In order to operate and maintain legacy systems, staff may need experience with older technology and programming languages, such as the Common Business Oriented Language (COBOL).[10] Agencies have had difficulty finding employees with such knowledge and may have to pay a premium for specialized staff or contractors. For example, we reported in May 2016 that the Social Security Administration (SSA) had to rehire retired employees to maintain its COBOL systems.[11]

  In addition, having a shortage of expert personnel available to maintain a critical system creates significant risk to an agency's mission. For instance, we reported in June 2018 that the IRS was experiencing shortages of staff with the skills to support key tax processing systems that used legacy programming languages.[12] These staff shortages not only posed risks to the operation of the key tax processing systems, but they also hindered the agency's efforts to modernize its core tax processing system.

  Further, having a shortage of personnel with necessary expertise can lead to delays in modernizing legacy systems. As we reported in February 2022, OPM's legacy financial system, Trust Funds Federal

[10]COBOL, which was introduced in 1959, became the first widely used, high-level programming language for business applications.

[11]GAO-16-468.

[12]GAO, *Information Technology: IRS Needs to Take Additional Actions to Address Significant Risks to Tax Processing,* GAO-18-298 (Washington, D.C.: June 28, 2018).

Financial System, was outdated and consisted of unsupported software. In fiscal year 2017, OPM created the Trust Funds Modernization Program to replace the legacy system. However, OPM had to extend the planned completion date of two project milestones by one year. OPM attributed the delay to a variety of reasons, including insufficient staff expertise regarding the legacy system.[13]

- **Increased costs.** The cost of operating and maintaining legacy systems increases over time. The issue of cost is linked to security risks, unmet mission needs, and staffing issues. Further, in an era of constrained budgets, the high costs of maintaining legacy systems could limit agencies' ability to modernize and develop new or replacement systems.

  For example, as we reported in October 2022, the Department of Education's Next Gen program was to develop and implement modernized technology, processes, and operations to improve its customer experiences and outcomes, across the entire student aid lifecycle.[14] In 2021, Education spent about $1.3 billion to maintain its current operating environment. However, the Next Gen program experienced several schedule delays that affected the agency's ability to retire two legacy systems. Maintaining one of these legacy systems longer than originally planned introduced more risk and would cost at least $26.5 million.

As we reported in June 2019, agencies cited several factors they consider prior to deciding whether to modernize a legacy system.[15] In particular, they reported evaluating factors such as the inherent risks, the criticality of the system, the associated costs, and the system's operational performance.

- **Risks**. Agencies may prioritize the modernization of legacy systems that have security vulnerabilities or software that is unsupported by the vendor.[16] However, limited system accessibility may also reduce

[13]GAO, *Information Technology: OPM Needs to Adopt Key Practices in Modernizing Legacy Financial System,* GAO-22-104206 (Washington, D.C.: Feb. 23, 2022).

[14]GAO, *Information Technology: Education Needs to Address Student Aid Modernization Weaknesses*, GAO-23-105333 (Washington, D.C.: Oct. 20, 2022).

[15]GAO-19-471.

[16]When computer systems or software are no longer supported, the vendor of the product ceases to provide patches, security fixes, or updates, leaving system vulnerabilities open to exploitation.

the need to modernize a legacy system. For example, air-gapped systems, which are systems that are isolated from the internet, may mitigate a legacy system's cybersecurity risk by preventing remote hackers from having system access.[17]

Conversely, we have also reported that air-gapped systems are not necessarily secure; they could potentially be accessed by other means than the internet, such as through Universal Serial Bus (known as USB) devices.[18] Even so, removing the threat of remote access is a mitigation technique used by agencies such as the Nuclear Regulatory Commission (NRC). According to NRC, the agency reduced the riskiness of using computers with unsupported operating systems by putting these computers on isolated networks or by disconnecting them from networks entirely.

- **Criticality**. Several agencies stated that they would consider how essential a legacy system is to their agencies' missions before deciding to modernize it. For example, the Department of Health and Human Services (HHS) stated that, when deciding to modernize a legacy system, it considers the degree to which core mission functions of the agency or other agencies are dependent on the system. Similarly, Department of Energy officials noted that the department is required to maintain several legacy systems associated with the storage of its nuclear waste.
- **Costs**. Agencies can consider the costs of maintaining a legacy system versus modernizing the system. For example, according to the Department of Veterans Affairs, there are systems for which a life-cycle cost analysis of the legacy system may show that the cost to modernize exceeds the projected costs to maintain the system. Similarly, the Department of Defense noted that, before deciding on a modernization solution, it is important to assess the costs of the transition to a new or replacement solution.

  An agency also may decide to modernize a system when there is the potential for cost savings to be realized with a modernization effort. For example, HHS stated that it may pursue the modernization of a

[17]See Department of Energy, Brookhaven National Laboratory, *Computer Security – Indirect Vulnerabilities and Threat Vectors (Air-Gap In-depth)*, BNL-114524-2017-CP (paper presented by Michael DePhillips at the International Conference on Physical Protection of Nuclear Material and Nuclear Facilities Conference, Vienna, Austria: November 2017).

[18]GAO, *Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities,* GAO-19-128 (Washington, D.C.: Oct. 9, 2018).

legacy system if the department anticipates reductions in operations and maintenance costs due to efficiencies gained through the modernization.

- **Performance**. Before making the decision to modernize, agencies can consider the legacy system's operational performance. Specifically, if the legacy system is performing poorly, the agency may decide to modernize it. For example, the Department of Transportation stated that, if a legacy system is no longer functioning properly, it should be modernized. In addition, HHS noted that the ability to improve the functionality of the legacy system could be a reason to modernize it.

Executive Branch and Congress Have Made Efforts to Modernize Federal IT

The executive branch and Congress have initiated several efforts to modernize federal IT, including the following:

- **National Cybersecurity Strategy.** In March 2023, the President released a strategy to elevate the cybersecurity posture of the federal government.[19] The strategy indicated that the Office of Management and Budget (OMB) would lead development of a multi-year plan to accelerate technology modernization. The plan would prioritize federal efforts on eliminating legacy systems that are costly to maintain and difficult to defend against sophisticated cyber threats. Specifically, the plan is to identify milestones to remove all legacy systems incapable of implementing the zero trust architecture strategy within a decade, or otherwise mitigate risks to those that cannot be replaced in that timeframe.[20]
- **Identification of High Value Assets**. In December 2018, OMB issued a memorandum that provided guidance regarding the

[19]The White House, *National Cybersecurity Strategy*, (Washington, D.C.: Mar. 1, 2023).

[20]Zero trust architecture is a cybersecurity approach that works on the "never trust, always verify" principle. It is intended to address the rapidly evolving security risks faced by IT systems worldwide. These risks include insider threats from employees who either deliberately or unintentionally create a security breach and new, more sophisticated and persistent threats from around the globe. For more information, see GAO, *Science & Tech Spotlight: Zero Trust Architecture,* GAO-23-106065 (Washington, D.C.: Nov. 18, 2022).

establishment and enhancement of the High Value Asset program.[21] It stated that the program is to be operated by DHS in coordination with OMB. The guidance required agencies to identify and report these assets (which may include legacy systems), assess them for security risks, and remediate any weaknesses identified, including those associated with obsolete or unsupported technology.[22]

- **Enactment of provisions commonly referred to as the Modernizing Government Technology (MGT) Act**. In December 2017, Congress and the President enacted a law to authorize the availability of funding mechanisms to improve, retire, or replace existing IT systems to enhance cybersecurity and to improve efficiency and effectiveness. The law, known as the MGT Act, authorizes agencies to establish working capital funds for use in transitioning from legacy systems, as well as for addressing evolving threats to information security.[23] The law also created the Technology Modernization Fund, from which agencies can obtain funds to retire and replace legacy systems, as well as acquire or develop systems.

  Subsequently, in February 2018, OMB issued guidance for agencies to implement the MGT Act.[24] The guidance was intended to provide agencies additional information regarding the Technology Modernization Fund, and the administration and funding of the related IT working capital funds. Specifically, the guidance allowed agencies to begin submitting initial project proposals for modernization on February 27, 2018.

[21]Office of Management and Budget, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, M-19-03 (Washington, D.C.: Dec. 10, 2018). This memorandum rescinded the previous guidance on High Value Assets, M-16-04 and M-17-09.

[22]According to OMB's December 2018 guidance, an agency may designate federal information or an information system as a High Value Asset when one or more of these categories apply to it: (1) the information or information system that processes, stores, or transmits the information is of high value to the federal government or its adversaries; (2) the agency that owns the information or information system cannot accomplish its primary mission essential functions within expected timelines without the information or information system; and (3) the information or information system serves a critical function in maintaining the security and resilience of the federal civilian enterprise.

[23]The MGT Act commonly refers to technology modernization provisions in the National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, Div. A, Title X, Subtitle G, 131 Stat. 1283, 1586-94 (2017).

[24]Office of Management and Budget, *Implementation of the Modernizing Government Technology Act*, M-18-12 (Washington, D.C.: Feb. 27, 2018).

In addition, in accordance with the MGT Act, the guidance provides details regarding a Technology Modernization Board, which is to consist of (1) the Federal Chief Information Officer (CIO) (Chair); (2) a senior official with IT development technical expertise from the General Services Administration; (3) a member of DHS's National Protection and Program Directorate;[25] and (4) four federal employees with technical expertise in IT development, financial management, cybersecurity and privacy, and acquisition, appointed by the Director of OMB.[26]

Congress initially appropriated $175 million in no-year funding to the Technology Modernization Fund through the annual appropriations process. On March 11, 2021, Congress and the President enacted legislation that appropriated an additional $1 billion to be available until September 30, 2025, to carry out the purposes of the fund.[27] In May 2021, OMB provided updated guidance to agencies regarding this $1 billion, which (1) prioritized projects that cut across agencies and address immediate cybersecurity gaps, and (2) allowed agencies to apply for a partial or minimal reimbursement of the funds provided.

According to OMB's website for the Technology Modernization Fund, the Technology Management Board had approved 40 projects across 24 federal agencies, totaling about $713 million, as of May 2023.[28] For example, the board approved about $13.9 million for the Department of Housing and Urban Development (HUD) to modernize a mainframe and five COBOL-based applications that were expensive to maintain. According to OMB's website, the investment began in August 2018

[25]The National Protection and Program Directorate was the DHS component responsible for addressing physical and cyber infrastructure protection. The Cybersecurity and Infrastructure Security Agency Act of 2018 renamed the National Protection and Program Directorate as the Cybersecurity and Infrastructure Security Agency and established a director and responsibilities for the agency.

[26]As of May 2023, these four employees were (1) the Federal Deposit Insurance Corporation's CIO, who is also the Chief Privacy Officer and Director of the Division of Information Technology; (2) the National Archives and Records Administration's CIO; (3) the National-Geospatial Intelligence Agency's Chief Technology Officer; and (4) the United States Digital Service's Administrator.

[27]American Rescue Plan Act of 2021, Pub. L. No: 117-2, Title IV, § 4011, 135 Stat. 4, 80 (2021).

[28]The MGT Act requires the Director of OMB to issue guidance on the administration of the fund and report the status of the awarded projects on a public website. OMB provides information on the status of awarded projects on the Technology Modernization Fund's website at https://tmf.cio.gov/.

and was closed out in August 2022, with no reported cost overruns and projected savings of about $8 million annually. According to HUD, securing these funds served as a catalyst inside the department and led to gathering strong support for this project. Without these funds, according to HUD, it would not have been able to pursue the project for several years.

However, we reported in December 2021 that, for numerous Technology Modernization Fund projects, agencies had yet to realize any cost savings, narrowed their respective projects' scopes resulting in reduced award amounts, and continued to use unreliable cost estimates.[29] We stated that, given the significant expansion in available funds, it was increasingly important for OMB and the General Services Administration to implement our prior recommendations from December 2019. This included developing and implementing a plan to fully recover operating expenses with fee collection and developing detailed cost estimating guidance.[30]

DHS Identified Three Legacy Systems and Developed a Modernization Plan for Its Most Critical System

In June 2019, we summarized 65 systems that the 24 Chief Financial Officers Act of 1990 agencies identified as their critical legacy systems in need of modernization.[31] Of the 65 systems, DHS identified three legacy systems in need of modernization and, at the time, these systems were about 6-11 years old.

Table 1 provides a list of the critical legacy systems that DHS identified, as of June 2019, as well as agency-reported system attributes, including the system's age, hardware's age, system criticality, and security risk. Due to sensitivity concerns, we substituted alphanumeric identifiers for

[29]GAO, *Technology Modernization Fund: Implementation of Recommendations Can Improve Fee Collection and Proposal Cost Estimates,* GAO-22-105117 (Washington, D.C.: Dec. 10, 2021).

[30]As described in the report, the Technology Modernization Fund received a significant increase in funding in March 2021 when the American Rescue Plan Act of 2021, Pub. L. No. 117-2, Title IV, § 4011, 135 Stat. 4, 80 (2021), appropriated an additional $1 billion to the fund. Prior to that time, the fund had received a total of $175 million through the annual appropriations process.

[31]GAO-19-471.

the system names and are not providing detailed descriptions. The identifiers in table 1 reflect how DHS's system names appeared in the 2019 report. GAO identified System 4 as one of the 10 most critical legacy systems in need of modernization.[32]

Table 1: Critical Legacy Systems in Need of Modernization According to DHS as of June 2019

System name[a]	Age of system, in years	Age of oldest hardware, in years	System criticality (according to DHS)	Security risk (according to DHS)
System 4	8–11[b]	11	High	High
System L	9	2	High	Moderately low
System M	6	1	High	Low

Legend:

Agencies reported the system criticality and security risk on a scale of 1 to 5 (with 5 being the most critical and the highest risk).

Low-1: According to the agency, system has low security risk or criticality.

Moderately low-2: According to the agency, system has moderately low security risk or criticality.

Moderate-3: According to the agency, system has moderate security risk or criticality.

Moderately high-4: According to the agency, system has moderately high security risk or criticality.

High-5: According to the agency, system has high security risk or criticality.

Source: GAO analysis of Department of Homeland Security (DHS) data. | GAO-23-106853

[a]Due to sensitivity concerns, we substituted an alphanumeric identifier for the system names. We assigned a number to identify each of the 10 most critical legacy systems in need of modernization and we assigned a letter or letters to identify the remaining 55 systems. The identifiers reflect how DHS's system names appeared in the 2019 report (GAO-19-471).

[b]The agency stated that the majority of the network's hardware was purchased between 2008 and 2011.

Given the age of the hardware and software in legacy systems, the systems' criticality to agency missions, and the security risks posed by operating aging systems, it is imperative that agencies carefully plan for their successful modernization. Documenting modernization plans in sufficient detail increases the likelihood that modernization initiatives will succeed. Our review of government and industry best practices for the

[32]To identify the 10 most critical legacy systems in need of modernization, we collected information on 65 of the most critical federal legacy systems and assigned point values based on system attributes, including a system's age, hardware's age, system criticality, and security risk. We then selected the 10 systems with the highest scores as the most critical legacy systems in need of modernization.

modernization of federal IT[33] stressed that agencies should have documented modernization plans for legacy systems that, at a minimum, include three key elements: (1) milestones to complete the modernization, (2) a description of the work necessary to modernize the legacy system, and (3) details regarding the disposition of the legacy system.

In June 2019, we evaluated agencies' modernization plans for the 10 most critical legacy systems. DHS was among eight agencies that lacked complete plans for modernizing their respective systems. Specifically, DHS's modernization plan for System 4 did not include milestones to complete the modernization or describe the planned disposition of the existing legacy system. Accordingly, we made a recommendation to DHS in a "limited official use only" version of the report to identify and document a modernization plan for this legacy system. In February 2022, DHS implemented our recommendation by updating its modernization plan to include milestones for implementing the replacement system and removing legacy hardware. By documenting its plan in sufficient detail, DHS increased the likelihood that this modernization will succeed.

DHS Made Progress in Addressing IT Modernization Recommendations, but Experienced Challenges in Meeting Program Goals

In the past several years, we reported on DHS's efforts to modernize and replace legacy systems that support various mission-critical activities, including financial management, biometric identity management, and

[33]General Services Administration, Unified Shared Services Management, *Modernization and Migration Management (M3) Playbook* (Aug. 3, 2016); and *M3 Playbook Guidance* (Aug. 3, 2016); American Technology Council, *Report to the President on Federal IT Modernization* (Dec. 13, 2017); Office of Management and Budget, *Management of Federal High Value Assets*, M-17-09 (Washington, D.C.: Dec. 9, 2016); American Council for Technology-Industry Advisory Council, *Legacy System Modernization: Addressing Challenges on the Path to Success* (Fairfax, VA: Oct. 7, 2016); and Dr. Gregory S. Dawson, Arizona State University, IBM Center for The Business of Government, *A Roadmap for IT Modernization in Government* (Washington, D.C.: 2018).

grants management.[34] Although DHS made progress by fully implementing 11 of 19 recommendations we made to help improve these modernization efforts, all three modernizations experienced challenges in meeting program goals. For example, all three modernizations experienced significant schedule delays up to several years. Further, some of the programs experienced cost overruns, performance issues, or had past modernization attempts that were not successful.

- ***DHS Financial Management.*** In February 2023, we reported that DHS has faced significant internal control and financial management systems deficiencies since the department's creation in 2003.[35] To address its financial management issues, DHS has attempted to develop a department-wide integrated and comprehensive financial management system for decades. In 2014, DHS began its third financial management system modernization attempt, which consisted of a decentralized, component-level approach.[36] We reported that DHS defined and implemented a tiered governance structure to provide oversight of its financial systems modernization programs, developed plans for modernizing specific financial systems, and established a process for lessons learned.

  For example, the Coast Guard deployed its new financial management system in December 2021 as part of a $510 million modernization program, and declared initial operational capability in June 2022. However, as we reported in February 2023, the Coast Guard was not able to declare full operational capability as expected in December 2022. Although DHS identified, documented, and tracked metrics to assess the Coast Guard's system deployment, the

[34]GAO, *DHS Financial Management: Actions Needed to Improve Systems Modernization and Address Coast Guard Audit Issues,* GAO-23-105194, (Washington, D.C.: Feb. 28, 2023); *Homeland Security: DHS Needs to Fully Implement Key Practices in Acquiring Biometric Identity Management System,* GAO-21-386, (Washington, D.C.: June 8, 2021); *FEMA Grants Modernization: Improvements Needed to Strengthen Program Management and Cybersecurity,* GAO-19-164, (Washington, D.C.: Apr. 9, 2019).

[35]GAO-23-105194.

[36]In fiscal year 2004, DHS first planned to develop an integrated and comprehensive financial management system department-wide. In fiscal year 2014, DHS revised its approach to focus its modernization efforts at the component level. In fiscal year 2018, DHS started to transition three components to a new financial management system, Financial Systems Modernization Solution (FSMS). These three components included Countering Weapons of Mass Destruction Office, Transportation Security Administration, and Coast Guard, and this effort is referred to as the Financial Systems Modernization (FSM)-Trio program.

department found that the system was not achieving expected capabilities. This was because the agency did not address and remediate known issues identified in operational testing. DHS's subsequent operational testing and evaluation of the system found that it was not effective, responsive, or reliable, and therefore could not proceed to full operational capability. In April 2023, DHS approved the Coast Guard's remediation plan to address outstanding issues. Based on this schedule, the program office expected to submit a revised acquisition program baseline in February 2024.

Additionally, FEMA and U.S. Immigration and Customs Enforcement (ICE) were in the planning phases of their financial systems modernization efforts. In November 2022, DHS awarded contracts for software licenses and planned to award contracts for system integration services for these components. Resolving deficiencies identified by testing before proceeding to the next phase in the acquisition process can help reduce the risk that future system modernization efforts at FEMA and ICE will not meet mission needs or expected capabilities. We made four recommendations to address these issues. DHS concurred and described actions it has taken and would take to address them.

- ***DHS Biometric Identity Management.*** In June 2021, we reported that DHS was using an outdated system for providing biometric identity management services (i.e., fingerprint matching and facial recognition technology services).[37] This system, known as the Automated Biometric Identification System or IDENT, became operational in 1994 and was to be replaced by a multi-billion dollar program known as the Homeland Advanced Recognition Technology (HART), which was initiated in 2016. We reported that DHS had initially expected to implement the entire program by 2021; however, no segments had been deployed by 2021. The program was estimated to cost about $4.3 billion and DHS planned to deploy the first increment in December 2021, and later increments in 2022 and 2024.

  Although the program had suffered continuing delays, the DHS CIO did not update the evaluation it had provided in November 2019, and continued to report the program as low risk on the IT Dashboard, a website showing, among other things, the performance and risks of agency IT investments. In May 2020, the Office of the CIO began developing a new quarterly process for assessing program risk, which

[37]GAO-21-386.

led to the CIO elevating HART's rating from low to high risk and reporting this rating to the IT Dashboard in November 2020. Though we found that the DHS CIO fulfilled applicable oversight requirements for high-risk IT programs by, among other things, conducting a TechStat review of HART, we concluded that the department's associated policy was outdated and not consistent with the processes the CIO was actually using.[38]

DHS had also implemented four of seven risk management best practices and partially implemented the remaining three. Further, of 14 selected IT acquisition best practices related to agreement management, project monitoring and control, and requirements management, DHS fully implemented seven and partially implemented the remaining seven. Accordingly, we made a total of seven recommendations to DHS, four of which have been fully implemented. Until DHS addresses the remaining three recommendations regarding monitoring contractor work products, program costs, and stakeholder involvement, the department risks experiencing further schedule delays and cost overruns. Additionally, DHS risks developing a system that may not meet its needs or those of its partner agencies.

In April 2023, we reported that HART had breached its cost and schedule goals in 2020 due to technical challenges and rework resulting from an overly complex, high-risk design, and disagreements with the contractor on program requirements.[39] DHS approved a new baseline for the program in May 2022, which focused on achieving initial operational capability by September 2023 (about 4 years later than originally planned).[40] Initial capabilities were to consist of the infrastructure necessary to operate HART as the biometric services system of record and the decommissioning of the legacy IDENT system. The program's full operational capability date was also delayed, from September 2021 to an unknown date that would be

[38]A TechStat review is an evaluation of high-risk IT investments to determine whether to terminate or turn around investments that are in danger of failing or are not producing results.

[39]GAO, *DHS Annual Assessment: Major Acquisition Programs Are Generally Meeting Goals, but Cybersecurity Policy Needs Clarification,* GAO-23-106701, (Washington, D.C.: Apr. 20, 2023).

[40]We have ongoing work reviewing the reliability of the HART program's 2022 cost and schedule estimates.

determined when DHS begins planning for future HART capabilities in 2023.

- ***FEMA Grants Management.*** In April 2019, we reported that FEMA initiated the Grants Management Modernization (GMM) program in 2015 to streamline and modernize its complex grants management IT environment.[41] That environment supported the award of billions of dollars in grants annually to help communities prepare for, mitigate the effects of, and recover from major disasters. The program was intended to replace 10 disparate legacy systems (several of which had been in operation for decades) that led to labor-intensive manual processes and an increased burden for grant recipients. FEMA had previously attempted to modernize its legacy grants management systems in 2008, through a program referred to as the Emergency Management Mission Integrated Environment (EMMIE). However, that program experienced significant implementation challenges, which resulted in a solution that was missing important capabilities.

  In our April 2019 report, we found that FEMA's endeavor to modernize its grants management environment had fully addressed seven of 11, and partially addressed the remaining four leading practices for effective business process reengineering, requirements management, and cybersecurity risk management. Specifically, the program did not fully address plans for new business processes, traceability of system requirements, or security control assessments. Additionally, the program's initial cost estimate of about $251 million did not reflect key technical assumptions that had changed. Further, the program's schedule did not meet leading practices for a reliable schedule. Of particular concern was that the program's fast approaching, final delivery date of September 2020 was not informed by a realistic assessment of development activities.

  FEMA has implemented seven of the eight recommendations we made to address these issues. The agency has also taken steps toward implementing the remaining recommendation to ensure that all security controls are fully tested, but has not yet demonstrated that it fully tested all controls. In April 2023, we reported that the program had rebaselined its cost and schedule in January 2021 and had requested additional schedule relief in August 2022 related to COVID-19.[42] As a result, FEMA planned to extend its full operational

[41]GAO-19-164.

[42]GAO-23-106701.

capability date to no later than March 2024, which would be three and one-half years later than originally planned.

In summary, our June 2019 report emphasized the need and importance for agencies to develop complete plans to modernize their most critical legacy systems. DHS has done so for its most critical system that was identified in 2019. It is vital for the department to continue planning how and when it will modernize its mission-critical legacy systems. Once the department establishes such plans, further steps are needed to ensure that efforts to modernize critical legacy IT systems are successfully carried out. While DHS has implemented many of our recommendations, implementing the remaining 8 for modernizing financial, biometric identity, and grants management systems would help ensure these critical legacy systems are successfully replaced.

Chair Hassan, Ranking Member Romney, and Members of the Subcommittee, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

GAO Contact and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact Kevin C. Walsh, Director of Information Technology and Cybersecurity, at (202) 512-6151 or walshk@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Jeanne Sung (Assistant Director), Paige Teigen (Analyst-in-Charge), Lauri Barnes, and Kim LaMore.

Post-Hearing Questions for the Record
Submitted to Eric Hysen
Chief Information Officer
U.S. Department of Homeland Security
From Senator James Lankford

"Securing the National: Modernizing DHS's Mission-Critical Legacy IT Systems"
Subcommittee on Emerging Threats and Spending Oversight
Senate Committee on Homeland Security and Governmental Affairs
May 31, 2023

Question#:	1
Topic:	Paper-Based Forms
Hearing:	Securing the Nation: Modernizing DHS's Mission-Critical Legacy IT Systems
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: How the Department is prioritizing the modernization of all its paper-based forms? Are all DHS online forms mobile responsive and fully compliant with section 4 (c) and section 3 (a) of the 21st Century IDEA?

Response: The U.S. Department of Homeland Security (DHS) is committed to improving the customer experience at every touch point between the public and the Department, including the access to and modernization of paper-based forms.

In March 2022, the Department launched the DHS Paperwork Reduction Act, Burden Reduction Initiative to eliminate 20 million of the over 190 million hours of administrative burden that DHS places on the public each year through its information collections, including paper-based collections. To accomplish this, the Department prioritized the approaches for Components to take, to include steps specifically intended to address existing paper-based collections:

- Simplifying and creating "short form" options;
- Enabling online submission of all forms, where appropriate;
- Accepting electronic or digital signatures;
- Ensuring that online forms are optimized for mobile devices;
- Conducting usability testing during the creation and revision process for all forms;
- Prepopulating forms and reusing existing known data and information;
- Using plain language;
- Reducing frequency of information collection; and
- Eliminating redundant or unnecessary collections.

DHS achieved burden reduction goals in May 2023 by using all of these approaches, most of which directly support 21st Century Integrated Digital Experience Act (21C IDEA). However, paper-based forms, including several not subject to the Paperwork Reduction Act, remain within the Department's inventory. As we make forms available electronically, some will continue to be available on paper so that individuals without the ability to use digital services are not deprived of or impeded in access to those digital services.

With respect to website modernization, the Department is focused on redesign and implementation of the US Web Design System as stipulated in section 3 (a) of 21C IDEA, to include enhanced mobile responsiveness for entire sites and any forms directly hosted on those sites.

DHS is prioritizing a new initiative to ensure DHS paper-based forms are modernized and that online forms are compliant with sections 4(c) and 3(a) of 21C IDEA. Specifics regarding this initiative are currently being finalized, and we anticipate being able to share details with the Committee by September 30, 2023.

Question: What is the timetable to ensure all websites, forms, and other paper-based and manual processes are fully compliant with 21st Century IDEA?

Response: While the Department has not yet determined an exact timetable for completion of the activities mentioned in the response to the previous question, we anticipate being able to share the scope and timeline of this effort by September 30, 2023. For example, DHS has over 230 Department-wide forms available online and is prioritizing full compliance of remaining paper-based forms with section 3(a) of the 21st Century IDEA.

Question#:	2
Topic:	Electronic Signature
Hearing:	Securing the Nation: Modernizing DHS's Mission-Critical Legacy IT Systems
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: Has the Department prioritized a plan to accelerate the use of electronic signatures as established under the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.)?

Response: The Department has prioritized electronic signature in specific use cases, including with respect to noncitizen encounters and our implementation of electronic or digital A-files[1] used upon initial encounters with noncitizens.

Although the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. § 7001 et seq., specifically pertains to interstate and foreign commerce, the Department supports this congressional mandate for our efforts as well. Thus, DHS is exploring how to modernize common business functions documenting exchanges with the public during the performance of our mission with the use of electronic signatures when appropriate.

[1] A-files are a series of records maintained on a person that document the person's immigration history. A-files are created when an application or petition for a long-term or permanent benefit is received or when an enforcement action is initiated. Currently, the information collected in the electronic files are based on certain CBP and ICE enforcement paper forms and other copies pertinent to the file. Once DHS has fully completed transitioning to an end-to-end electronic processing state, all electronically created immigration documents associated with enforcement encounters will be available through Unified Immigration Portal.

Question#:	3
Topic:	Paper-Based System
Hearing:	Securing the Nation: Modernizing DHS's Mission-Critical Legacy IT Systems
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: The immigration system is primarily paper-based, even though we've had TurboTax since the early 2000s. What impact does this have on our economy? What impact does this have on our national security? Please share any assessment on this issue with the Committee.

Response: Historically, the immigration process had been paper-based and largely manual. However, the Department has made tremendous progress in transitioning to more digital, automated, and interoperable processes.

For example, through the Southwest Border (SWB) Technology Integration initiative, DHS is digitizing and automating many of the immigration processes, as well as ensuring that our front- line agents and officers are spending less time on manual paper-driven processes. Examples of progress include:

- Mobile Intake, which enables initial data capture at encounter rather than requiring a return to station, has saved U.S. Border Patrol (USBP) agents 29,000 hours since April 2022.
- Case Acceptance System (CAS) allows U.S. Customs and Border Protection (CBP) to digitally refer a case to U.S. Immigration and Customs Enforcement (ICE) for a custody determination instead of communicating requests via multiple emails and phone calls.
    - This system enables ICE Enforcement and Removal Operations (ERO) officers to accept and process more cases, with over 505,000 CBP transfer requests submitted as of July 27, 2023, through CAS.
- The Alternatives to Detention (ATD) micro app, which streamlines ICE's ATD enrollment process, has reduced enrollment time by about 68 percent and ensured consistent and transparent enrollment data between ICE and its ATD vendor.
- Electronic A-files, which were first deployed by CBP Office of Field Operations in El Paso in July 2022 and have since been deployed to six SWB USBP sectors and all SWB Field Offices, have resulted in:
    - Over 1,100 electronic files currently created per day (based on recent data),
    - $25 in shipping costs saved per file, and
    - 20-30 minutes of CBP processing time saved per file.

Question#:	4
Topic:	USCIS IT Modernization Plan
Hearing:	Securing the Nation: Modernizing DHS's Mission-Critical Legacy IT Systems
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: Have you assessed the outdated IT at USCIS? What steps do they need to take to modernize? Please share any USCIS IT modernization plan with the Committee.

Response: Yes, the Department has assessed the IT systems at U.S. Citizenship and Immigration Services (USCIS).

Section 4103 of the Emergency Stopgap USCIS Stabilization Act, Title I, Div. D of Public Law (P.L.) 116-159 (8 U.S.C. 1103 note) required that the Secretary of Homeland Security provide a 5-year plan to enable electronic filing for all applications and petitions for immigration benefits, accept electronic payments at all filing locations, issue correspondence electronically, and improve processing times for all immigration and naturalization benefit requests.

Since delivery of the *Section 4103 Plan Pursuant to the Emergency Stopgap USCIS Stabilization Act*, dated September 7, 2021, USCIS has made measurable progress toward enabling electronic filing and digital processing capabilities.

USCIS has the capability to electronically intake 69 percent of the total Fiscal Year (FY) 2023 forecasted receipts of applications, petitions, and other requests for benefits, as well as online payments, if customers choose online filing. USCIS has steadily increased the availability of forms for online filing from the 35 percent reported in the 2021 Section 4103 Plan.

Additionally, USCIS personnel are now able to process 88 percent of their workload electronically, which represents an increase from the 69 percent capacity reported in the 2021 Section 4103 Plan.

USCIS receives applications, petitions, and requests for benefits which are categorized within four Lines of Business (LOB):

- *Citizenship*: Persons applying for naturalization, certificates of citizenship, and all other citizenship-related benefits.
- *Humanitarian*: Refugee, asylum, parole, Temporary Protected Status, deferred action, and other protections.
- *Immigrant*: Lawful Permanent Residents, employment-and family-based adjustment of status, and immigrant investors.
- *Nonimmigrant*: Student, visitor, and employment-based nonimmigrants.

Question#:	4
Topic:	USCIS IT Modernization Plan
Hearing:	Securing the Nation: Modernizing DHS's Mission-Critical Legacy IT Systems
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

The table below depicts the progress made since the FY 2021 Section 4103 Plan, organized by LOB, to achieve end-to-end electronic processing, defined by USCIS as the ability to electronically intake submitted applications, petitions, and requests for benefits, accept payments electronically, complete the adjudication process from start to finish electronically, and correspond with customers electronically:

Current State of End-to End Electronic Processing Capability		
Line of Business	**% Electronic Capability**	
	2021 Section 4103 Plan	**As of FY 2023 Q2**
Citizenship	100%	100%
Humanitarian	67%	92%
Immigrant	62%	84%
Non-Immigrant	17%	54%

Notably, the following capabilities to achieve end-to-end electronic processing have been delivered since FY 2022:

		Form		Capability
FY 2022	**Q1**	I-589	Application for Asylum and for Withholding of Removal (e-filing channel)	End-to-end electronic processing - e-file intake and electronic adjudication *(Soft Launch)*
		I-765 c11	Application for Employment Authorization (*Operation Allies Welcome)*	Electronic adjudication *(Emergent Requirement)*
		I-129 H-1B	Petition for Nonimmigrant Worker H-1B Specialty Occupations	Electronic adjudication for H-1B non-cap cases
		I-907	Request for Premium Processing Service	Electronic adjudication for Premium H-1B non-cap case requests

Question#:	4
Topic:	USCIS IT Modernization Plan
Hearing:	Securing the Nation: Modernizing DHS's Mission-Critical Legacy IT Systems
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

	Q2	I-821D	Consideration of Deferred Action for Childhood Arrivals[2]	E-file intake
		I-765 c33	Application for Employment Authorization Deferred Action for Childhood Arrivals[2]	E-file intake
	Q3	I-129 H-1B	Petition for Nonimmigrant Worker H-1B Specialty Occupations	Electronic adjudication for H-1B visa cap cases
		I-907	Request for Premium Processing Service	Electronic adjudication for Premium H-1B visa cap case requests[3]
		I-134	Declaration of Financial Support *(Uniting for Ukraine)*	End-to-end electronic processing - e-file intake and electronic adjudication *(Emergent Requirement)*

[2] I-821D and I-765 are bundled for concurrent filing.

[3] Congress mandates a numerical limit on the number of new H-1B visas, or status grants, issued per fiscal year (FY) at 65,000. This is commonly referred to as the "regular cap." Congress also created an exemption of 20,000 new visas or status grants for beneficiaries with a qualifying U.S. master's degree or higher (advance degree exemption or master's cap). Collectively, the master's cap and regular cap are referred to as the "cap."

Question#:	4
Topic:	USCIS IT Modernization Plan
Hearing:	Securing the Nation: Modernizing DHS's Mission-Critical Legacy IT Systems
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Form				Capability
FY 2023	Q1	I-134A	Declaration of Financial Support *(Expanded to Venezuela, Cuba, Haiti, and Nicaragua)*	End-to-end electronic processing - e-file intake and electronic adjudication *(Emergent Requirement)*
		I-590	Registration for Classification as Refugee	Electronic adjudication
		N/A	Credible Fear / Reasonable Fear Electronic Process	Electronic adjudication
		I-765 c11	Application for Employment (Zero Fee for Afghan and Ukrainian Parolees)	End-to-end electronic processing - e- file intake and electronic adjudication
		I-589	Application for Asylum and for Withholding of Removal (e-filing channel)	E-file intake (Official Launch)
		I-765 c08	Application for Employment Authorization Pending Asylum Applicant	E-File intake
		N-600	Application for Certificate of Citizenship (Armed Forces)	E-File intake
		I-130	Petition for Alien Relative	USCIS Online Account Services (I-130 Personalized Processing Times)
	Q2	I-907	Request for Premium Processing Service (I-765 C03)	End-to-end electronic processing - e-file intake and electronic adjudication (Premium I-765 C03 Requests)
		I-131	Application for Travel Document	E-file intake
		I-907	Request for Premium Processing Service	Electronic adjudication for Premium I-140 Requests (Upgrades)
		I-751	Petition to Remove Conditions on Residence	Electronic adjudication

Question#:	4
Topic:	USCIS IT Modernization Plan
Hearing:	Securing the Nation: Modernizing DHS's Mission-Critical Legacy IT Systems
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

USCIS is actively engaged in increasing the scope of retrospective digitization of USCIS records to support efficiencies in both adjudication and record retention. For example, USCIS converts paper submissions to electronic content during the intake processing for certain forms. Applicants can also submit certain benefit requests using the agency's online account platform. Each of these methods result in robust simultaneous efforts to address high-priority pending immigration benefit requests through increased electronic accessibility for adjudication. These processes also help reduce the agency's physical storage footprint and increase record retention agility for multiple immigration product lines.

Question: What systems modernization processes has USCIS undertaken over the past year? What specific steps have been taken to move toward electronic processing? Please describe all new steps toward the electronic processing of immigration benefits that have been implemented from FY2021 to the present to the Committee in detail.

Response: Please see above response for efforts undertaken by USCIS to move toward full electronic processing. In addition, USCIS coordinated with its DHS partners to implement significant modernization efforts over the past year:

- Unified Immigration Portal (UIP) is an interagency solution between CBP, USCIS, ICE, the U.S. Department of Justice (DOJ), and the U.S. Department of Health and Human Services (HHS).
    - Credible fear data is now ingested into UIP to improve data sharing among CBP, ICE and USCIS for Expedited Removals (ER) processing.
- DHS has developed electronic A-number issuance and the capability for downstream partners to push content into an electronic A-file.

Question#:	5
Topic:	Electronic Processing Plans
Hearing:	Securing the Nation: Modernizing DHS's Mission-Critical Legacy IT Systems
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: Please describe all planned steps toward electronic processing for the remainder of FY2023 and the duration of FY2024 in detail.

Response: The Department's digital A-File team, which includes representation from all DHS immigration components, streamlined the manual and resource-intensive paper A-file process through the creation of electronic A-files. This development allows for continued use of electronic processing by downstream partners. The Department creates over 1,100 electronic A-files per day in this way. This effort required extensive systems integration and coordination among CBP, ICE, and USCIS.

USCIS will continue to make more forms available for end-to-end electronic processing, as resources and emergent circumstances allow.

For additional information related to electronic processing, please see the response for 4a.

Question#:	6
Topic:	Interoperability
Hearing:	Securing the Nation: Modernizing DHS's Mission-Critical Legacy IT Systems
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: What steps have been taken to ensure that USCIS' immigration records and processing systems are interoperable with CBP systems? With ICE's systems? With HHS Office of Refugee Resettlement systems? With DOJ Executive Office for Immigration Review systems? Please describe in detail all steps that have been taken toward interoperability among these agencies' systems from FY2021 to the present. Please also describe in detail all planned steps toward interoperability among these agencies' systems for the remainder of FY2023 and FY2024.

Response: Since FY 2021, the Department has been engaging in a comprehensive effort to coordinate the development and to ensure the interoperability of immigration records in the digital space. This effort has included the creation and joint solutioning of an electronic A-file architecture and constant touchpoints to ensure lockstep progress. Some examples that reflect this cooperation include:

- UIP is an interagency solution between CBP, USCIS, ICE, DOJ, and HHS. Through use of a single platform, UIP connects disparate systems, improves cross-agency collaboration, and increases data transparency across the immigration lifecycle. UIP allows officers to see data and electronic content and creates reports by integrating data and providing visibility of near real-time information across multiple agencies.
- The tri-component electronic A-File requires extensive systems integration and coordination between CBP, ICE, and USCIS, including development of significant supporting functionality by component partners, such as:
    - electronic and digital signatures on forms;
    - integration of person-centric identity comparison and validation;
    - digital A-number issuance; and
    - the ability to identify and apply digital processes in internal case management systems, and the exchange and sharing of information and content among all components.
- The electronic A-file creation requires the electronic issuance of an A-Number and the creation of an electronic record that will eventually store all official documents related to the individual. The A-file follows the noncitizen through the immigration lifecycle. More than one third of the electronic A-files created by CBP, approximately 1,100 per day, are now electronic.

DHS has automated the credible fear referral between ICE and USCIS by fully digitizing the case file and, thus, eliminating the need for a paper A-file to be transferred from ICE to USCIS.

Question#:	6
Topic:	Interoperability
Hearing:	Securing the Nation: Modernizing DHS's Mission-Critical Legacy IT Systems
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

DHS plans to continue toward interoperability among these agencies' systems. Planned steps include:

- Continue progress toward end-to-end electronic A-file processing implementation for remaining major processing dispositions;
- Continue to expand electronic Notice to Appear (NTA) creation;
- Build out additional dispositions based on operational priority for each component, in coordination with the SWB Technology Group (Parole, voluntary return, ER);
- Implement scheduling integration for credible fear interviews at USCIS/ICE/CBP; and
- Digitize all required detention forms that are inputted into the A-File.

Question: As we in Congress consider how to address the immigration system, particularly in light of the border crisis, what resources are needed to improve the interoperability of the Departments' border security and immigration-related systems?

Response: DHS appreciates Congress' support for immigration system modernization and interoperability.

- USCIS requested, and was granted, expanded authority to use discretionary funds for asylum adjudication purposes in the FY 2023 Budget and increase in the number of asylum applications completed from a goal of 50 thousand in FY 2022 to 65 thousand in FY 2023.
- USCIS was appropriated an additional $133 million in FY 2023 for asylum processing. The FY 2024 Budget requests an increase of $156.5 million for asylum adjudications in support of asylum processing.
- The FY 2023 appropriations include funding to support technology improvements to the immigration system, including:
    - $9 million to CBP for UIP to address current challenges regarding immigration data sharing. This investment will focus on continued development of the UIP platform, which will allow the program to complete the backend data-mesh to enable all partners to quickly publish and access accurate real time data.
    - $6.0 million for ICE T-8. This investment will focus on continued productivity improvements that will have significant positive impacts across each phase of ERO's mission. T-8 is an ERO portfolio of projects established for building data management tools to reduce redundant processes and enhance officer decision- making.

In addition, DHS has used the Technology Modernization Fund since FY 2021 to:

Question#:	6
Topic:	Interoperability
Hearing:	Securing the Nation: Modernizing DHS's Mission-Critical Legacy IT Systems
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

- accelerate the SWB work related to integrating disparate, siloed immigration processing systems;
- automate, digitize and streamline manual (often paper) processes; and
- enhance front-line efficiency and engagement with noncitizens at the SWB.

Finally, with the Consolidated Appropriations Act, FY 2022, Section 538, Congress authorized DHS to establish a Nonrecurring Expenses Fund (NEF) for IT modernization and facilities infrastructure improvements. DHS anticipates the initial amount of available NEF funding to be relatively small due to funds control requirements for expired funds but anticipates increased funds will be available over time. The NEF allows unobligated balances of expired one- and multi-year discretionary funds to be transferred into the fund. Over time these transfers should increase as additional years of expired funds are de-obligated from contracts and additional unobligated balances expire. The NEF will serve as a potential avenue for enhancing interoperability of the Department's border security and immigration-related systems.

Should the Department need additional funds not available through one of these methods, DHS will request such funding through the budget process.

Question: CBP, ICE, and USCIS' systems are not interoperable. What would it take to make these systems interoperable?

Response: The SWB technology improvement effort, initiated in February 2021, makes interoperability among CBP, ICE and USCIS a goal, along with:

- integrating disparate, stove-piped immigration processing systems;
- automating, digitizing and streamlining manual (often paper) processes; and
- enhancing front-line efficiency and engagement with the noncitizens they encounter.

For example, UIP is an interagency solution between CBP, USCIS, ICE, DOJ, and HHS. UIP connects relevant data from agency information technology systems through the UIP portal across the immigration lifecycle, providing a comprehensive view of an individual's known immigration history. The system provides near real-time data across agencies in multiple visual and reporting format options.

In addition, the CAS, which allows CBP to refer a case to ICE for a custody determination electronically rather than waiting hours for ICE to come pick up a paper file and make a custody determination, enhances interoperability, and enables ERO officers to accept and process more expedited removal cases.

Question#:	6
Topic:	Interoperability
Hearing:	Securing the Nation: Modernizing DHS's Mission-Critical Legacy IT Systems
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Please see responses above for additional examples. DHS looks forward to continuing the discussion of these and other initiatives with the Subcommittee as we work together to build upon this progress.

Question#:	7
Topic:	Technology Modernization Fund
Hearing:	Securing the Nation: Modernizing DHS's Mission-Critical Legacy IT Systems
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: Since its creation in 2017, the TMF has received $1.225 billion to fund modernization projects. The TMF Board awarded DHS $50 million for the Southwest Border Technology Integration Program project (expected completion Sept. 2024), and $26.9 million for the Homeland Security Information Network project (expected completion Nov. 2024).

What is the application process like to receive TMF funds? What administrative hurdles does DHS face in accessing that money?

Response: Agencies submit technology modernization proposals to the Technology Modernization Fund (TMF) Board through a two-phased approval process. First, the agency submits an Initial Project Proposal, which serves as a pre-screening for Board approval. If approved to continue, the agency next submits a Full Project Proposal, which includes a more comprehensive description of the proposal, discrete project milestones, and a proposed schedule.

In the case of the SWB Technology Integration and the DHS Homeland Security Information Network initiative, DHS teams also delivered presentations to the Board prior to project award.

DHS has found TMF to be a viable option for information technology modernization, consistent with the intent of Congress. However, DHS faces an administrative hurdle associated with the enactment of the FY 2022 Consolidated Appropriation Act, Division F, Title V, Section 539 (a) (1-3), which requires the DHS Head of Agency signature on all notifications related to new proposals. This provision introduces additional administrative lead time into the process, which the project teams work to mitigate.

Question: Are any current projects held up due to inability to access TMF funds?

Response: No.

Question#:	8
Topic:	Remote Border Technology
Hearing:	Securing the Nation: Modernizing DHS's Mission-Critical Legacy IT Systems
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Question: The President's budget requested $305.5 million for non-intrusive inspection systems, and prior legislative and administrative efforts under President Trump also sought to improve our capabilities along the border. However, agents and officers in remote locations on the border often lack the systems and technologies necessary to carry out their border security mission.

What impacts does our technological posture have on our border security mission?

Response: Technology has been a critical component in how the Department is addressing the challenges at the border. The advancements in Internet of Things technology, with remote visibility into small footprints, has provided emerging opportunities to better protect our borders. Artificial intelligence and machine learning and automated video data information understanding have transformed what was manually impossible before into actionable intelligence within seconds at the fingertips of agents in the field, and in real-time, on a handheld device. The ability to share large data sets with pinpointed relevancy as needed across agencies is made possible by technology enhancements.

CBP uses a wide range of non-intrusive inspection systems and capabilities at our nation's ports of entry. This allows for remote locations to use a variety of tools, such as large and small scale inspection systems.

With continued support from Congress, CBP, in coordination with our partners, will continue to deploy critical resources to the border and refine the effectiveness of our detection, interdiction, and identification capabilities to combat transnational threats and the entry of illegal drugs into the United States.

Question: What does DHS need to consider to modernize these systems?

Response: As previously noted, expanding connectivity infrastructure along the SWB involves various challenges. For example my office recently collaborated with the Cybersecurity and Infrastructure Security Agency (CISA) to conduct a geospatial analysis that identified several geographic areas along the border with limited or no access to communications infrastructure. To overcome some physical geography challenges, DHS will need to partner with other federal agencies and private industry to enhance communication capabilities along the border.

Question: How would you address remote locations and the lack of the physical infrastructure necessary to facilitate the use of modernized systems along certain aspects of the border?

Question#:	8
Topic:	Remote Border Technology
Hearing:	Securing the Nation: Modernizing DHS's Mission-Critical Legacy IT Systems
Primary:	The Honorable James Lankford
Committee:	HOMELAND SECURITY (SENATE)

Response: CBP is looking at solutions to address technology issues in remote locations. $8 million of Procurement, Construction, and Improvement funding enacted for USBP Border Security Technology in Fiscal Year 2023 was allocated to Seamless Integrated Communications (SIC) efforts on the SWB. SIC funding will be used for communication upgrades that will enable bidirectional data flow from sensors and phones with the CBP network, the Team Awareness Kit, and other sensor systems that improve shared awareness, officer safety, and effectiveness. Interoperability will permit multicomponent and multisensory communications and future enhanced joint border operations and will be the enabler for autonomous sensors and mesh network systems. Procurement of two terminals, three radio frequency kits, one antenna deployment kit, and five sensor network access points per area of responsibility (AOR) will support a tactical integrated network within remote communications-deprived areas of the Southern Border. SIC technology procurement will enable expansion to ten USBP Station AORs.

Post-Hearing Questions for the Record
Submitted to Eric Hysen
Chief Information Officer
U.S. Department of Homeland Security
From Senator Jon Ossoff

"Securing the National: Modernizing DHS's Mission-Critical Legacy IT Systems"
Subcommittee on Emerging Threats and Spending Oversight
Senate Committee on Homeland Security and Governmental Affairs
May 31, 2023

Question#:	9
Topic:	Upgrade IT
Hearing:	Securing the Nation: Modernizing DHS's Mission-Critical Legacy IT Systems
Primary:	The Honorable Jon Ossoff
Committee:	HOMELAND SECURITY (SENATE)

Question: The legacy information technology systems of the Department of Homeland Security pose a significant risk to the department's data security. Outdated technology leaves the department's data, including sensitive information related to financial and human resources management, vulnerable to the actions of malicious cyber actors.

What steps is the Department of Homeland Security taking to upgrade Department information technology systems to ensure that the data under Department management is protected and what additional resources and authorities are needed from Congress to continue adapting these systems to an evolving cyber threat environment?

Response: The Department chooses to confront cybersecurity risk—such as end-of-life and unsupported products—through an iterative approach to modernization. This approach uses modern tools like the Unified Cybersecurity Maturity Model (UCMM) to characterize and contextualize *actual* risk posed and allow DHS to validate areas of low risk and focus precious resources in areas where it provides greater impact to securing and improving our services and systems. Since 2022, DHS has leveraged the UCMM framework to prioritize immediate remediation activities, resulting in the closure of 64 percent of overdue actions at DHS Headquarters in a year's time. The framework's use has since been expanded in FY 2023 and is routinely part of operational decisions to guide cybersecurity maturity improvements across Component Agencies. We also modernize legacy systems by implementing the standards outlined in the DHS Zero Trust architecture as well as the updated protections required by Executive Order (EO) 14028, "*Improving the Nation's Cybersecurity.*" We further buttress these efforts through services to DHS Components focused on risk management, including the DHS Cybersecurity Service Provider program that standardizes component security operations centers and network operations centers across the Department, as a best practice for the entire

government. DHS has been focused on upgrading software/hardware of systems that cannot fully meet the requirements outlined in Executive Order 14028 which include multi-factor authentication, encryption at rest, or encryption in transit. These upgrades have resulted in the Department reaching over 95 percent compliance with the EO requirements.

End-of-life products pose particular cybersecurity risks and vulnerability issues as they lack available patching or adequate support. America's adversaries and cyber criminals know to look at legacy systems for such exposed vulnerability. Despite our leadership role within the interagency in this area, DHS recognizes that our efforts can always be improved and welcomes the opportunity to discuss any further areas of interest or newly contemplated authorities with the Subcommittee.

Question#:	10
Topic:	Risks to Privacy
Hearing:	Securing the Nation: Modernizing DHS's Mission-Critical Legacy IT Systems
Primary:	The Honorable Jon Ossoff
Committee:	HOMELAND SECURITY (SENATE)

Question: I remain concerned about the potential risk posed by DHS law enforcement and intelligence activities to the civil liberties and privacy of my constituents. These risks grow when personally identifiable information is processed and stored on outdated legacy information technology systems.

What steps is the Department of Homeland Security taking to ensure department information technology systems, particularly those which facilitate information collection and sharing among law enforcement and intelligence agencies, can appropriately mitigate risks to privacy?

Response: The Department has established policies and directives to ensure the protection of sensitive information within DHS Components. These policies limit access to authorized users, processes, and devices, ensuring DHS systems are configured to provide only essential capabilities and to restrict the use of non-essential functions, thereby minimizing potential risks. DHS implements various access control requirements, including robust account management and least privilege access for job roles.

Legacy systems that collect and share information among law enforcement and intelligence agencies are subject to the strictest control requirements in DHS's implementation of the risk management framework required by the Federal Information Security Modernization Act of 2014. Given the extremely sensitive nature of the information these systems manage, they require 35 percent more security controls be established and verified before the system is authorized for use. Furthermore, these systems are continuously monitored for anomalous events which, should they occur, are prioritized and addressed by DHS security operations.

The Department has also prioritized collaboration with all components to successfully implement key cybersecurity initiatives necessary to protect DHS sensitive data and infrastructure such as implementation of Encryption of Data at Rest and in Transit for all DHS information systems, cloud modernization, establishing Zero Trust Architecture through incremental implementation of Zero Trust capabilities, hardening Identity and Credential Access Management (ICAM) capabilities, and implementing the DHS Supply Chain Risk Management (SCRM) program. As of the end of the third quarter of FY 2023, the Department has achieved over 95 percent compliance with the requirements of EO 14028.

Through its rigorous privacy compliance process, the DHS Privacy Office assesses the privacy risks of new or amended DHS IT systems, including proposed uses of data, data security, retention, and dissemination, and develops mitigation strategies to be implemented by the relevant component. These mitigation strategies are typically explained in DHS Privacy's published Privacy Impact Assessments. If there is a breach to a DHS system, the DHS Chief

Question#:	10
Topic:	Risks to Privacy
Hearing:	Securing the Nation: Modernizing DHS's Mission-Critical Legacy IT Systems
Primary:	The Honorable Jon Ossoff
Committee:	HOMELAND SECURITY (SENATE)

Privacy Officer and Component Privacy Officers work closely with the Chief Information Officer to identify and respond to privacy and computer security incidents to mitigate harm to DHS-maintained assets, information, personnel, and the public. Privacy incidents involving personally identifiable information are also subject to strict Congressional reporting standards and timelines provided through Office of Management and Budget guidance, as well as potential notice to affected individuals. As discussed above, DHS has a robust process to assess privacy risks and implement mitigation strategies that are incorporated into Privacy Impact Assessments which are posted at www.dhs.gov/privacy.

Question#:	11
Topic:	SCIF Technology
Hearing:	Securing the Nation: Modernizing DHS's Mission-Critical Legacy IT Systems
Primary:	The Honorable Jon Ossoff
Committee:	HOMELAND SECURITY (SENATE)

Question: Recent intelligence leaks highlight the importance of the infrastructure and processes which we utilize to process, store, and disseminate classified information. This includes the information technology systems that the Department of Homeland Security uses to store and disseminate sensitive information internally and with federal partners.

What is the state of information technology at the Department of Homeland Security's secure compartmented information facilities?

Does the age or condition of these information technology systems pose a risk to the security of these facilities and to the security of classified information stored, processed, and distributed by the Department of Homeland Security?

Response: DHS has its own Top Secret Network infrastructure, managed per National Security Standards, processes, and procedures. DHS is further implementing guidance within the *National Security Memorandum/NSM-8*.

Question: Does the age or condition of these information technology systems pose a risk to the security of these facilities and to the security of classified information stored, processed, and distributed by the Department of Homeland Security?

Response: There is no known risk associated with the age or condition of the IT systems on this network.

Question#:	12
Topic:	DHS Offices
Hearing:	Securing the Nation: Modernizing DHS's Mission-Critical Legacy IT Systems
Primary:	The Honorable Jon Ossoff
Committee:	HOMELAND SECURITY (SENATE)

Question: What offices or DHS components have responsibility for ensuring the secure implementation and management of Top Secret network accesses, communications, and facilities? [You may respond classified.]

Response: The Department's Office of Intelligence and Analysis (I&A), the DHS Office of the Chief Security Officer (OCSO), and my office share responsibility in this area. OCSO accredits the physical protections of the sensitive compartmented information facilities (SCIFs); I&A authorizes and manages the use of secure compartmented information (SCI) in SCIFs, and provides accreditation and authorizes, ensures compliance, and oversight to all IT at the Top Secret Sensitive Compartmented Information for the Department. My office authorizes and manages all IT at the Top Secret collateral level and below and provides network operations and security center monitoring for the network.

Post-Hearing Questions for the Record
Submitted to Charles R. Armstrong
Chief Information Officer
Federal Emergency Management Agency
U.S. Department of Homeland Security
From Senator Jon Ossoff

"Securing the National: Modernizing DHS's Mission-Critical Legacy IT Systems"
Subcommittee on Emerging Threats and Spending Oversight
Senate Committee on Homeland Security and Governmental Affairs
May 31, 2023

Question#:	1
Topic:	Inhibiting Upgrades
Hearing:	Securing the Nation: Modernizing DHS's Mission-Critical Legacy IT Systems
Primary:	The Honorable Jon Ossoff
Committee:	HOMELAND SECURITY (SENATE)

Question: The age and state of DHS and FEMA information technology systems inhibits the quality and timeliness of service to my constituents, including time-sensitive federal disaster assistance, and undermines trust in government's capacity to solve problems.

What factors have inhibited the Department's ability to upgrade and improve its grants managements and disaster assistance support systems?

Response: As the Federal Emergency Management Agency (FEMA) seeks to upgrade its systems, we must recognize and plan for the fact that many of our systems are interconnected and provide support to communities and survivors around the clock. These systems have interdependencies with each other that need to be carefully planned as migration and modernization occurs to avoid data loss, security issues, or service disruption. This planning, while necessary and appropriate, also introduces delays into the process.

There are several factors that inhibit FEMA's ability to upgrade and improve its grants management and disaster assistance support systems. The following points illustrate the existing challenges that the agency faces:

- Dependence on modifications to legacy FEMA Office of the Chief Financial Officer financial management systems remains a risk and a challenge to both grants management and disaster assistance support system upgrades. Program management offices from

these related modernization efforts regularly collaborate to identify and remediate potential risks to understand interdependencies and integrate modernization schedules.

- Requirements for multi-factor authentication and zero trust need to be balanced against other agency modernization priorities, such as cloud migration, agile adoption, and modern technical architecture and software delivery approaches. These outcomes compete for resources and influence the overall timeline. Modernization programs are working closely with the U.S. Department of Homeland Security (DHS) and FEMA cybersecurity offices to appropriately prioritize and implement these requirements without further delaying modernization.
- Moving existing systems off aging on-premises hardware to the cloud will improve sustainability and interoperability, but has added a layer of complexity to the overall modernization effort for grants and disaster assistance. Ongoing collaboration with the modernization programs will ensure understanding and remediation of potential risks.

Question#:	2
Topic:	FEMA IT Improvements
Hearing:	Securing the Nation: Modernizing DHS's Mission-Critical Legacy IT Systems
Primary:	The Honorable Jon Ossoff
Committee:	HOMELAND SECURITY (SENATE)

Question: What IT-oriented efforts are underway to improve the quality and timeliness of service for those Americans in need of federal disaster assistance?

What additional authorities and resources are needed from Congress to enable the necessary improvements to FEMA IT systems?

Response: FEMA is standing up a Digital Customer Experience (DCX) team within the Office of the Chief Information Officer (OCIO). This team is currently supporting the rollout of streamlined disaster assistance registration by performing usability testing with the public, designing a phased deployment, and ensuring adequate observability and testing. The DCX team is also evaluating internal OCIO processes to identify areas to automate and streamline the approval and compliance steps related to IT upgrades to enable FEMA teams to modernize IT systems more efficiently.

The team will provide research, design, and development support to program offices to make applying for disaster assistance easier, more efficient and more personalized. This effort directly supports the President's Management Agenda Priority 2 to "Deliver excellent, equitable, and secure Federal services and customer experience. Increase experience quality to be on par with

leading consumer experiences. Reduce burden for government's customers and improve trust in government."

Some of the projects the DCX team is supporting now and in the coming months include:

- Streamlining the survivor-facing Individual Assistance application on DisasterAssistance.gov.
    - Conducting usability study with members of the public to identify usability issues that could impact survivors applying for disaster assistance
    - Planning for a post-launch usability study to guide upcoming enhancements to improve the survivor experience.
- Consulting on the user experience of an updated public-facing website for Transitional Sheltering Assistance that will provide a mobile-first website to the public with modern search and filtering functionality.
- Research and design for modernizing the accompanying call-center side of the Individual Assistance application. This will support FEMA staff to provide support to survivors applying over the phone.
- Scoping and customer experience strategy for the development of a modernized, survivor data management system.

FEMA also recently onboarded a US Digital Services team of product managers, engineers, and service designers. They are facilitating and scaling up cross-agency work with Small Business Administration as part of Streamlining Disaster Assistance Life Experience Project.

Additionally, FEMA is folding many legacy federal assistance systems into the Grants Management Modernization initiative with the full operational capability milestone targeted for the 2nd quarter of FY 2024. Modernizing these legacy systems and ensuring they are able to take advantage of scalability in the cloud will enable FEMA to provide timely and high-quality disaster financial assistance.

○