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.