Information Technology Strategic Plan

U.S. Department of Homeland Security

FY2024 – 2028

Homeland Security

DHS Information Technology (IT) Strategic Plan

FY2024 2028

Message from the Chief Information Officer

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 seaports, to businesses importing goods into our country, to disaster survivors applying for assistance and immigrants applying for benefits. An increasing portion of those interactions occur through our information technology systems. The DHS IT community plays a more critical role than at any time in our Department's history to executing our mission. Within this context, I am pleased to share the Department's IT Strategic Plan for Fiscal Years 2024 – 2028. Over the next five years, this plan will guide DHS information technology by serving as the touchstone for our modernization efforts. Specifically, the DHS IT community will:

- Invest in our workforce – attracting, hiring, developing, and retaining diverse technology talent to meet expanding needs, helping employees develop new skills in emerging technical fields, and making DHS a place where IT professionals can do meaningful work, grow their careers, and bring their authentic selves to work every day;
- Lead in our responsible use of Artificial Intelligence to secure the homeland and defend against the malicious use of this transformational technology against our systems and data, while ensuring that our use is rigorously tested to avoid bias and disparate impact, safeguards privacy, and is clearly explainable to the people we serve;
- Strengthen our data management, governance, sharing, and integration to improve our operations, better identify and respond to constantly evolving threats, and build trust;
- Improve Customer Experience to transform and innovate our delivery of services to advance mission execution, increase access to services and informed compliance with security and law enforcement, and provide more equitable, accessible, and effective services to the public;
- Build modern, effective software and retire costly legacy systems through implementing agile development, continuous integration and delivery, and shared enterprise services; and
- Lead the rest of the Federal Government by example in our own cybersecurity practices including zero trust adoption and IT supply chain security.

Technology is constantly evolving, and any multi-year IT plan is out of date the second it is finalized. This strategic plan is no exception. So, while I look forward to working with my colleagues across the Department to implement this plan, I am even more excited to learn with them and continuously improve our approach in the years to come.

ERIC N HYSEN Digitally signed by ERIC N HYSEN
Date: 2023.09.26 15:57:41 -04'00'

Eric Hysen, Chief Information Officer
Department of Homeland Security

Introduction

DHS Mission and Core Values

DHS has a vital mission: *With honor and integrity, we will safeguard the American people, our homeland, and our values*. This responsibility is carried out by over 260,000 dedicated employees who perform diverse duties, including aviation and border security, promoting trade and travel for economic security, emergency response, and cybersecurity.

DHS is committed to embodying the relentless resilience of the American people, ensuring a safe, secure, and prosperous homeland in a constantly evolving global environment.

To adapt to the ever-changing landscape, the DHS IT community will equip the Department with secure and resilient capabilities. This will also promote interoperability, information sharing, and collaboration among DHS and its partners.

The Department will responsibly employ emerging technologies and maintain a highly skilled workforce to provide the capabilities needed to support the mission. DHS will work with its partners to implement best practices and solutions to adapt to technological advancements and foster cohesion across the Department.

DHS IT Strategic Plan FY2024 – 2028

The DHS IT Strategic Plan FY2024-2028 enables the Department to set goals and support cross-functional and cross-organizational priorities to achieve our mission. This plan is intended as a guide to help define goals and objectives for the DHS workforce and support delivery of modern, innovative, and efficient services and solutions to safeguard the homeland.

The DHS IT Community will align to these strategic goals to support our mission during the next five years. The plan will be executed collaboratively across DHS Headquarters, Agencies & Offices

The backbone of this plan and the most critical factor to its success will be the 5,000 talented and committed professionals that comprise the DHS IT workforce. This strategy ensures we continue to invest in our talented workforce and prepare our colleagues for the future in an ever-changing IT landscape. Moreover, much of this modernization plan originated from countless conversations, meetings, town halls, and site visits with the IT workforce across the Department.

DHS IT Strategic Goals and Descriptions

Goal 1: Invest in the DHS IT Workforce

The DHS IT community is made up of thousands of talented, dedicated, and mission-driven technology professionals. They are our greatest asset, but they are also too few. DHS will attract, hire, develop, and retain diverse technology talent to meet expanding needs. We will invest in developmental and training opportunities to help employees develop new skills in emerging technical fields. Through these efforts, we will make DHS a place where IT professionals can do meaningful work, grow their careers, and bring their authentic selves to work every day.

Objectives

1.1. Build a diverse, equitable, and inclusive workplace: DHS strives to attract individuals across all levels of the DHS IT workforce, including senior leadership positions, that represent the diversity of the populations we serve. We will expand partnerships with diverse academic institutions, professional organizations, and communities and strengthen internship, rotation, and developmental programs that promote equitable access to career advancement for all employees. We will also expand our distributed and remote hiring to reach more diverse qualified candidates across the country.

1.2. Create department-wide training programs: DHS is designing, implementing, and continuously improving department-wide training programs for the IT community. We will establish the 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. This approach fosters collaboration and enhances the exchange of knowledge and best practices, creating a learning community extending beyond formal training sessions. Finally, DHS is integrating these IT training programs with DHS workforce development plans to reinforce long-term succession planning and individual career growth.

1.3. Fully leverage modern hiring practices: DHS is committed to fully adopting the Cybersecurity Talent Management System (CTMS). Launched in November 2021 and currently being used to fill critical skill gaps in some Components, DHS plans to implement CTMS across all Components. Furthermore, DHS will expand the applicability of CTMS as a hiring mechanism for a wider array of cybersecurity professionals, to include support for data science, Artificial Intelligence, and other emerging technologies. DHS will supplement these efforts by fully exercising the hiring authorities and flexibilities available under Title 5.

1.4. Enhance cohesion within the IT community: In line with the Secretary's priority to strengthen Department-wide cohesion, we will build a variety of mechanisms to ensure every DHS IT employee feels connected to and supported by the broader Department-wide IT community. We will implement regular IT Community Town Halls, Symposia, and awards programs to bring the entire community together. We will establish and promote communities of practices across components and implement digital platforms to enhance collaboration. Finally, we will strengthen our IT councils, including the DHS Chief Information Officer (CIO), Deputy CIO, Chief Information Security Officer, Chief Technology Officer, Chief Data Officer, IT Operations, and Business Management Councils, as forums for senior collaboration and decision-making.

Goal 2: Responsibly Use Artificial Intelligence to Transform Operations

During his April 21, 2023, State of Homeland Security address, Secretary Mayorkas stated that "Our Department will lead in the responsible use of AI to secure the homeland and in defending against the malicious use of this transformational technology. As we do this, we will ensure that our use of AI is rigorously tested to avoid bias and disparate impact and is clearly explainable to the people we serve." The DHS IT community will play a critical leadership role in this transformation.

Objectives

2.1. Adopt AI technologies: DHS will test and implement AI technologies to improve mission operations and service delivery. Generative AI, Machine Learning (ML), Computer Vision, and other AI enhance the Department's capabilities in core areas: threat detection, critical infrastructure security, and decision-making. Incorporating the use of these technologies across DHS mission spaces will increase efficiencies, realize cost savings, improve decision-making, enhance intelligence collection, streamline citizen services, improve fraud detection, transform intelligence analysis, and improve DHS operations.

2.2. Ensure safe, trustworthy, and responsible use: DHS will continue to prioritize safe, trustworthy, and responsible use of AI and be transparent with the public on how AI is used throughout the Department. We will establish rigorous standards for testing AI systems, to include measuring for unintended algorithmic bias, evaluating quality, relevance, and usage rights of data on which AI models are trained, and ensuring algorithms are effective for their intended uses. We will partner with the Department's Privacy and Civil Rights and Civil Liberties offices, as well as other stakeholder communities to strengthen the governance and oversight of AI systems in line with rapidly evolving law, guidance, and best practices.

2.3 Develop enabling AI infrastructure: DHS will explore and develop common infrastructure to support rapid and effective AI implementations across different use cases. This may include shared deployments of foundation models or common services to connect to external models, along with building operations pipelines to prepare, test, and deploy data for use in machine learning. We will update policies to promote responsible AI adoption and explore common procurement actions to give all parts of the Department access to modern AI technologies. We will ensure that our AI implementations are interoperable across the Department and minimize vendor lock-in in a rapidly evolving space.

2.4. Build an AI-ready workforce: DHS will build skills in data science and AI across the IT workforce and focus on hiring experts in these critical fields. More critically, we will ensure all DHS employees build AI literacy. Just as every DHS employee must know basic cybersecurity best practices, they will also need to understand AI capabilities and weaknesses. This will enable them to harness AI systems effectively and responsibly and proactively defend against potential AI threats.

Goal 3: Leverage Data as a Strategic Asset

Sharing information and data is at the heart of why DHS was established as a Department. While respecting individuals' civil rights, civil liberties, and privacy, we must strengthen how we share data internally among DHS Agencies & Offices and with external partners across the public and private sectors to improve our operations and better identify and respond to constantly evolving threats. Improving our data management practices is also critical to make the Department's data

AI-ready. Where appropriate, we will increase transparency in our data to build greater trust with the American people.

Objectives

3.1. Integrate data across disparate systems and data sources: With such a diverse set of missions and complex architecture of existing systems and processes, any effort to consolidate DHS data in a single data warehouse or hub will fail. Instead, DHS seeks to drive data integration through mission-focused data sharing platforms that leverage open standards and operate across both legacy and modernized systems while respecting data ownership within individual Agencies & Offices. This approach is already showing results in efforts including the Southwest Border Technology Integration Program, Integrated Multi-Domain Enterprise, and National Vetting Center.

3.2. Strengthen data inventory & discovery: While DHS will not seek to consolidate data into a single or small number of data warehouses, we will ensure that our data is fully cataloged and discoverable by internal and (where appropriate) external users. We will continue to expand our data inventory with a focus on automating identification, making metadata useable, complete, and accurate, publication of datasets wherever possible, and making it easier to find, access, and update inventory records.

3.3 Ensure adherence to records retention requirements: DHS data also includes official Government records. This data must be managed to preserve the historical record, promote accountability, and enhance public trust. In line with the Federal Records Act, OMB Circular A 130, and the National Archives and Records Administration guidelines, our IT and Data teams will collaborate closely with the Department's Records Officer communities. This partnership aims to seamlessly integrate records management, retention, and disposition mandates into every phase of the DHS information life cycle.

3.4. Refine mission-aligned data governance: Rather than taking a one-size-fits-all approach, DHS has developed a data governance method grounded in 13 different data domains that represent different parts of the Department's mission. We will continue to improve governance practices to ensure the enterprise data management lifecycle promotes accurate, accessible, understandable, and secure data. We will ensure that statistical data governance and operational data governance are synchronized. We will implement governance mechanisms that prioritize and safeguard the decision-making processes essential for the success of our missions. In doing so, we will leverage experiences from successful domain-specific governance programs, such as the Immigration Data Integration Initiative, as examples for other areas.

3.5. Partner to drive evidence-based policymaking: In line with the Foundations for Evidence-Based Policymaking Act of 2019, the DHS IT and Data communities will develop strong working relationships with the Department's Statistical Official and Evaluation Officer communities to strategically plan for evidence building and data management while preserving statistical and scientific integrity. We will share insights and findings to improve how we collect data and measure results. We will coordinate and assess data programs, policies, and procedures. We will improve our data governance and processes based on evidence and statistics.

***3.6. Publish more usable open data and APIs*:** As we build our internal data management and sharing capabilities, we will seek to make that same data available externally where appropriate. We will engage with the open data community to understand how DHS data is useful to them and seek to align our efforts to ensure data and Application Programming Interfaces (APIs) best meet their needs, including publishing more machine-readable, structured data.

Goal 4: Improve Customer Experience and Transform Service Delivery

DHS interacts with millions of customers every year through digital, in-person and combined touchpoints. We are committed to improving Customer Experience (CX) to transform and innovate our delivery of services to advance mission execution, increase access to services, like informed compliance with security and law enforcement, and provide more equitable, accessible, and effective services to the public. This effort extends to our internal customers as well: Tools and systems for DHS personnel must be accessible, useful, usable, easy to learn, and efficient to use. Customer experience design, including accessibility beyond Section 508 compliance, ensures that touchpoints with the public bring about trust and confidence in our services.

Objectives

4.1. Transform critical services: Each DHS Agency & Office will identify their most critical services, conduct user research to understand the lived experiences of their customers, and iteratively work towards concrete CX improvements in the near term while building towards longer term transformations. For services that share customers across Agencies & Offices, such as Trusted Traveler Programs, we will partner to develop shared transformation roadmaps that respect the full lifecycle of a customer's interactions across DHS. Concurrently, we will establish relationships with internal and external communities that promote transparency, accountability, and collaboration.

4.2. Use accountability and compliance processes to improve accessibility and usability and reduce public burden: DHS will continuously improve our processes for ensuring our actions with internal and external customers are compliant with applicable laws including Section 508 of the Americans with Disabilities Act, the Paperwork Reduction Act (PRA), and the 21st Century Integrated Digital Experience (IDEA) Act. Moreover, DHS intends to exceed what is legally required and make our services equitable, accessible, and usable. Accessibility and human-centered practices more broadly must be a part of designing policies, processes, and interactions from the very beginning rather than a compliance exercise at the end. Finally, we will continue to reduce the administrative burden we place on the public each year, through continuing to streamline collections under the PRA and modernizing DHS forms to ensure they are compliant with the IDEA Act.

***4.3. Build and strengthen a human-centered decision-making culture*:** DHS will establish CX literacy and fluency across the Department through experiential training, coaching, and building modern tools. We will promote and support human-centered methods, such as user research and usability testing. Program and IT teams will build skills in human-centered design methods and service delivery best practices. DHS will continue and expand ADA 508-related programs, including the Trusted Tester program. We will establish, deliver, and promote plain language guidance and training.

***4.4. Mature and measure CX organizations and practices*:** DHS will build and expand centralized CX functions at DHS Headquarters, Agencies & Offices, starting with our High Impact Service Providers. We will develop a CX maturity model based on best practices from across government and private sector and use it to measure our progress. We will track and publish metrics on CX across the Department.

Goal 5: Build Modern, Effective Software

Historically, agencies across the Federal Government, including DHS, took a "big bang" approach toward software development and IT modernization. Government staff spent years gathering requirements, awarding a large contract to a single systems integrator to build to those exact requirements and test extensively against them. In theory, a 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 waterfall approach leads to modernization programs going over budget and behind schedule at alarming rates. DHS rejects this approach in favor of a more incremental, iterative, and measured strategy based on private sector best practices that enable us to build modern software systems.

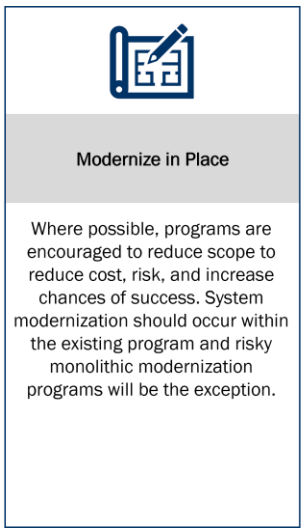
Objectives

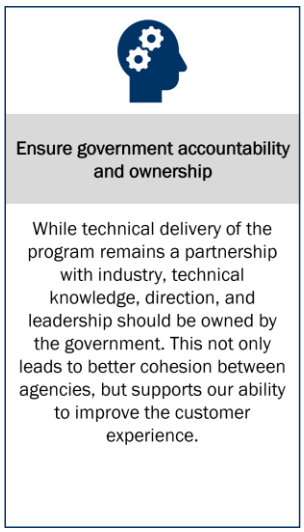
5.1. Modernize in place: We will no longer take the "big bang" approach with IT modernization. This monolithic approach creates unnecessary risk and provides little value to our customers. Instead, we will adopt the practice of modernizing in place. We will build smaller, discrete system functions and deploy these new capabilities within existing environments. This enables us not only to deliver new capabilities to our customers faster, but design systems for interoperability.

5.2. Ensure government accountability and ownership: The Department, not any one vendor, must serve as the integrator ultimately responsible for successful delivery of a software system. We depend on our industry partnerships but require strong technical expertise in federal service to oversee contract deliverables and ensure results.

5.3. Research, develop, test, and deploy iteratively and continuously: While agile development, DevOps, and Continuous Integration and Continuous Delivery (CI/CD) have become widely adopted terms across DHS, we have more work to do to embrace the true intent of these concepts. We will ensure that all new software efforts start with a strong foundation of user research and deploy minimum viable products to users within months of kicking off. Projects will then adopt continuous cycles of user research, development, usability and software testing, and deployment to maintain flexibility to changing mission and customer needs. We will reject "AgileFall" - when seemingly iterative methodologies are used on the surface, but a program still relies on a long-term, pre-defined schedule. We will increase our use of trusted open source software and reusable government code and expand our contributions back to the open source community, including reuse of our own code across the Federal Government.

5.4. Use enterprise services: DHS will continue to invest in enterprise services in network and security operations, cloud infrastructure, developer tools, common software platforms, identity, and other areas and adopt these services across IT systems. We will explore building new enterprise services as new technology patterns and needs emerge. In doing so, we will reduce duplication across IT programs to reduce complexity and cost and strengthen system reliability, effectiveness, and security.





Goal 6: Secure Our Systems & Data

As the Department that is responsible for cybersecurity of the Federal Civilian Executive Branch and critical infrastructure, DHS has a special responsibility to lead the rest of the Federal Government by example in its own cybersecurity practices. Cybersecurity is a shared responsibility across the IT community, and everyone involved in designing, building, and using our systems has a role to play.

Objectives

6.1. Advance cybersecurity capabilities through the Unified Cybersecurity Maturity Model (UCMM): DHS will continue to refine the UCMM as a tool to understand organizational cybersecurity maturity and risk posture and identify specific areas of concern. We will further incorporate the UCMM into resource planning to enable all DHS Agencies & Offices to increase their maturity levels.

6.2. Secure IT supply chains: DHS will continue to mature cybersecurity supply chain risk management practices such as vendor due diligence assessments and software assurance processes. We will fully implement our authorities under the SECURE Technology Act to remove companies from the Department's IT supply chains and support DHS' government-wide responsibilities via the Federal Acquisition Security Council. As we continue to evolve our processes in a rapidly changing legal and policy environment, we will ensure close coordination with our industry partners to avoid surprises and unintended consequences, and we will seek to incentivize the right practices in the private sector rather than issue blanket mandates.

***6.3. Implement Zero Trust architecture*:** Cybersecurity is not an all-or-nothing approach: we must embed security into all parts of the IT organization, network architecture, and software development lifecycle. We are not so naïve as to think that we will prevent every breach, but instead must also look to limit the potential impact of breaches that do occur. DHS will bolster cybersecurity measures and minimize vulnerabilities through the stringent application of access controls and adaptive security protocols. By upholding the principles of least privilege and dynamic response, we will continue to reduce the attack surface and potential fallout from breaches and ensure that our security strategies remain agile and effective against emerging threats.

6.4. Partner to increase cybersecurity resilience: DHS cannot secure our systems and data alone – we rely on our partners. We will continue to expand the Hack DHS bug bounty program and vulnerability disclosure policy to benefit from private security researchers and hackers identifying

vulnerabilities in our systems before our adversaries can exploit them. We will strengthen our partnerships with and contributions to the open source software community to improve collective security. Finally, we will increase transparency with our industry partners to learn and strengthen security practices together.

Applying the Strategic Plan to DHS IT Modernization

DHS is committed to a comprehensive IT modernization approach that strategically integrates statutory CIO authorities.[1] Our goal is to seamlessly infuse IT modernization priorities into existing DHS decision-making processes, in alignment with the objectives set forth in the Modernizing Government Technology Act of 2017 and this strategic plan. To do so, the Department will implement the following methodology:

1. ***Identify modernization opportunities:*** We will continuously assess our IT portfolio to identify potential modernization prospects. We are enhancing our portfolio management processes by integrating methodologies, such as Capital Planning Investment Control and DHS Program Health Assessments along with the Unified Cybersecurity Maturity Model. Concurrently, we are aligning these efforts with Federal Information System Management Act evaluations. By doing so, we gain a holistic perspective of our IT portfolio, allowing us to identify candidates for modernization.
2. ***Prioritize critical projects:*** As modernization candidates are identified, we will use established governance bodies, such as the DHS CIO Council, to prioritize those that offer the most tangible benefits to cybersecurity, customer experience, and employee experience and effectiveness.
3. ***Fund projects through innovative means:*** To support risk-based decision-making, DHS is aligning future IT budget requests with the DHS UCMM framework. We will issue annual IT resource planning guidance and approve funding for projects that are in line with our modernization objectives. In cases where funding is necessary outside of the regular budget cycle, we will use the DHS Nonrecurring Expenses Fund [2] and other innovative funding models, such as the Technology Modernization Fund.
4. ***Build and Deploy:*** We will execute modernization projects by deploying the strategies in this plan. We will hire and develop a world-class IT workforce that can exercise necessary technical oversight of our vendors. We will modernize in place and start small, employing agile development and continuous integration and delivery to rapidly deliver value for our customers. In summary, DHS' IT modernization approach is grounded in a comprehensive, well-coordinated effort that integrates statutory authorities, identifies opportunities, prioritizes initiatives, aligns resources, and invests in the DHS IT workforce to effectively

[1] CIO authorities are enumerated within the: Paperwork Reduction Act of 1980, as amended, 44 U.S.C §§ 3501-3521; Clinger-Cohen Act of 1996, 44 U.S.C. §§ 11101-11704; Federal Information Security Modernization Act of 2014 (FISMA), 44 U.S.C. §§ 3551-3558; and Federal Information Technology Acquisition Reform Act (FITARA), Public Law 113-291, "Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015," Title VIII, "Acquisition Policy, Acquisition Management, and Related Matters," Subtitle D, as codified in relevant part at 40 U.S.C. §11319.

[2] The Nonrecurring Expenses Fund (NEF), as authorized by the Consolidated Appropriations Act, 2022 (Public Law 117-103), Title V, Section 538, enables DHS to transfer unobligated balances of expired discretionary funds for nonrecurring information technology (IT) modernization and facilities infrastructure improvements.

serve our mission to safeguard the nation. This commitment allows us to achieve our IT modernization goals while effectively serving our mission to safeguard the nation.

The Way Forward

Implementation of this modernization plan relies on two of the greatest assets at the Department's disposal—the DHS IT workforce and our external partners, including industry, the public, and Congress. Through the Federal Information Technology Acquisition Reform Act and other key legislation, as well as funding flexibilities and support for priorities identified through this document, DHS has tools and means to achieve this plan's objectives. The Department will use the roadmap from this IT Strategy to enter the next phase in our modernization journey. This plan will become a touchstone for IT fiscal decisions, performance plans for senior leaders, and policy changes. With this path forward for IT modernization at DHS, we will continue to refine our efforts to best support our missions and workforce.

Homeland Security