OFCIO
OFFICE OF THE FEDERAL CHIEF INFORMATION OFFICER

2024 IMPACT REPORT

OFFICE OF MANAGEMENT AND BUDGET

OFCIO
OFFICE OF THE FEDERAL CHIEF INFORMATION OFFICER

BACKGROUND

This document provides a high-level view of progress made by the Office of the Federal Chief Information Officer (OFCIO) during the Biden-Harris Administration. To learn more about OFCIO and our mission, visit whitehouse.gov/omb/management/ofcio.

Note that this document was compiled based on data available at the time of publication. It represents a snapshot in time and — since we are continually working to deliver for the American people — some of the information represented in this report may have changed since publication. To stay up-to-date with the latest developments in Federal information technology (IT), visit cio.gov.

ACKNOWLEDGEMENTS

This document was developed by OFCIO and highlights the work of our office in partnership with key stakeholders.

Photograph: *OFCIO team members on the Navy Steps at the Eisenhower Executive Office Building in November 2024.*

Table of Contents

2 Letter from the Federal Chief Information Officer

4 Tech Policy Timeline

6 Cybersecurity

10 Technology Modernization and Data

14 Digital Service Delivery

17 Artificial Intelligence

20 Power of Partnerships

23 Resources

LETTER FROM THE FEDERAL CHIEF INFORMATION OFFICER

Technology underpins the Federal Government's ability to secure its systems and data from adversaries and deliver services to the American people that meet today's expectations.

This is the view from the Federal Chief Information Officer's (CIO) office window at the Eisenhower Executive Office Building, just steps away from The White House. A sign reads "proceed as if success is inevitable" — a powerful reminder that we need to be thinking big on behalf of the millions we're here to serve — the American people.

Over the last four years, the Biden–Harris Administration has boldly seized the power of technology to transform and modernize Government in the face of unprecedented challenges — including a global pandemic and a string of sophisticated cyberattacks that tested the resilience of our systems. Due to this Administration's work and leadership, we've emerged stronger, more resolute, and more innovative than ever before.

Technology modernization is a bipartisan issue and rests on a foundation that must be continually secured and built upon so our Nation can deliver on its critical missions. At OFCIO, we've spearheaded an ambitious "whole-of-government" strategy that gives agencies the mandate needed to drive digital transformation across Government and requires results. We optimized our approach to Federal IT by implementing human-centered policy design, which requires collaborating with agencies and engaging technologists and key stakeholders from the start.

Through this coordinated, technology-forward policy approach, we're empowering agencies to deliver a simple, seamless, and secure digital experience for the American people.

The public deserves a simple, seamless, and secure experience when they interact with our Government.

Our four key priorities include:

Bolstering Cybersecurity. Defending our digital world is essential to ensuring the safety and security of our Nation. By adopting modern security practices into our policies, we're positioning agencies to effectively safeguard critical systems and data against those who seek to do us harm. We've strengthened our cyber defenses and the American people are more protected today as a result. We continue to work across the Federal ecosystem to ensure we have the 21st century cyber workforce needed now and in the future.

Modernizing Technology and Leveraging Data. We can't lead as a Nation if our technology is falling behind, so we're accelerating IT modernization through innovative initiatives like the Technology Modernization Fund (TMF). The TMF gives agencies additional ways to deliver services to the American public more quickly, better secure sensitive systems and data, and maximize the impact of taxpayer dollars. Simultaneously, we must ensure that the data that resides in Federal systems is secure, accurate, actionable, and accessible to power intelligent Government operations and citizen experiences.

Advancing the Use of Emerging Technologies like Artificial Intelligence (AI). The Administration's Executive Order (EO) on *the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* is ensuring the United States leads the way in responsible innovation. We're not just implementing AI — we're setting the global standard for its use. Federal agencies are partnering with top tech talent to develop AI solutions — to make Government work for the American people.

Improving Digital Service Delivery. More than ever, digital experience is central to Federal agencies' mission delivery and our Government's ability to serve the American people. That means we are championing the responsible use of emerging technologies like AI to streamline operations and deliver more personalized Government experiences. Ongoing investments are enabling agencies to deliver intuitive, accessible digital services that meet the public's expectations and restore their trust in Government.

Through continued collaboration, innovation, and the courage to work differently, this work will transform the Federal landscape and ensure our Government delivers for every American today and into the future. The American people deserve nothing less.

Clare Martorana

Clare A. Martorana
Federal Chief Information Officer
Office of Management and Budget
The White House

TECH POLICY TIMELINE

This timeline shows a high-level view of OMB's tech policy progress across administrations. Milestones align with four key priorities: Cybersecurity, Technology Modernization and Data, Digital Experience and Service Delivery, and Artificial Intelligence. Use the timeline and legend to track progress over time.

PRE 2021

Federal Information Security Modernization Act (FISMA): Outlines information security authorities for OFCIO and Federal Government
- **Established FISMA Metrics + Issued Annual FISMA Report to Congress**

Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure (SECURE) Technology Act: Establishes Federal Acquisition Security Council (FASC)

21st Century Integrated Digital Experience Act (IDEA): Requires Federal Government to improve digital experience for the public

Modernizing Government Technology (MGT) Act: Establishes Technology Modernization Fund (TMF)
- **Issued M-18-12, *Implementation of the MGT Act***
- **10 TMF investments totaling $65.6 million**

Federal Information Technology Acquisition Reform Act (FITARA): 1st major overhaul of Federal IT in almost 20 years

EO 13960 on *Promoting the Use of Trustworthy AI in the Federal Government:* Requires inventory of Federal AI use cases

EO 13859 on *Maintaining American Leadership in AI:* Establishes Federal strategies to strengthen U.S. capabilities in AI

Federal Risk and Authorization Management Program (FedRAMP): Establishes secure, modern adoption of cloud services by Government

Foundations for Evidence-Based Policy Making Act: Modernizes Federal data management practices

AI in Government Act: Creates AI Center of Excellence

2021

EO 14028 on *Improving the Nation's Cybersecurity:* Paradigm shift to modern security practices such as zero trust
- **Issued M-21-30, *Protecting Critical Software Through Enhanced Security Measures***
- **Issued M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents***
- **Issued M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response***

Stood up FASC, issuing the FASC Final Rule which outlines FASC procedures on authorities to recommend exclusion and/or removal orders

American Rescue Plan Act: Historic $1 billion to TMF to invest in projects that boost cybersecurity defenses, address urgent IT modernization challenges, and improve the delivery of COVID-19 relief and public-facing digital services
- **8 TMF investments totaling $362.9 million**

EO 14058 on *Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government*

Established Zero Trust Metrics + Issued Annual FISMA Report to Congress

Issued annual OMB *Circular A-11, Section 55* for agency reporting on IT investment portfolios

2022

Issued M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*

Issued M-22-09, the Federal Zero Trust Strategy, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*
- **Agencies submitted initial zero trust implementation plans**

Issued 1st joint ONCD-OMB guidance on cyber funding priorities for the Federal budget

Published 1st Federal Cybersecurity Progress Report

17 TMF investments totaling $208.8 million

Convened FASC stakeholders across Government, establishing governance, maturity models, and guidance on Supply Chain Risk Assessments via NIST 800-161 Appendix E

Published Federal IT Operating Plan to highlight how to maximize impact of Federal IT funding

LEGEND

Blue / : Cybersecurity
Red / : Technology Modernization and Data
Green / : Digital Experience and Service Delivery
Yellow / : Artificial Intelligence

Shades of color (i.e., lighter or darker hues) represent related milestones within the same priority area. Milestones can be connected across different years. For example, FISMA is blue because it's under "cybersecurity," and all FISMA-related entries are the same shade of blue.

Note: This timeline is not intended to be comprehensive and there may be additional milestones not depicted on this timeline.

2022

Quantum Computing Cybersecurity Preparedness Act and National Security Memorandum 10, *Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems*
- **Issued M-23-02, *Migrating to Post-Quantum Cryptography* (PQC)** initiating steps for agencies to migrate to PQC
- **Established interagency PQC Migration Working Group**

Advancing American AI Act: Promotes the use of AI across Government, codifies aspects of EO 13960, and requires AI use case inventories
- **Managed AI Use Case Inventory** to promote transparency around how Government uses AI

Issued Annual FISMA Report

Issued annual OMB *Circular A-11, Section 55* for agency reporting on IT investment portfolios

AI Training Act: Requires OMB to establish or provide an AI training program for the Federal acquisition workforce

FedRAMP Authorization Act: Codified FedRAMP

2023

Issued M-23-16, *Update to Memorandum M-22-18*

Convened White House Multifactor Authentication (MFA) Modernization Symposium with industry and Government leaders to support advances in phishing-resistant MFA

13 TMF investments totaling $128.1 million

Issued M-23-22, *Delivering a Digital-First Public Experience*

Issued M-23-10, *The Registration and Use of .gov Domains in the Federal Government*

Issued M-24-08, *Strengthening Digital Accessibility and the Management of Section 508 of the Rehabilitation Act*

Managed and expanded AI Use Case Inventory + metrics

Convened the inaugural government-wide AI Training series with over 4,800 participants from 78 Federal agencies

EO 14110 on *the Safe, Secure, and Trustworthy Development and Use of AI*

Matured operations of FASC by increasing interagency information sharing

Issued joint ONCD-OMB guidance on cyber funding priorities for the Federal budget

Issued Annual FISMA Report

Published Federal Cybersecurity Progress Reports

No TikTok on Government Devices Act
- **Issued M-23-13, *"No TikTok on Government Devices" Implementation Guidance***

National Cybersecurity Strategy

Issued annual OMB *Circular A-11, Section 55* for agency reporting on IT investment portfolios

2024

Agencies submitted updated zero trust implementation plans and maturity assessments

CDO and CISO Council published *Federal Zero Trust Data Security Guide*, led by OMB

Convened inaugural gathering of international government digital leaders at The White House

Established Digital Experience Council to coordinate digital delivery efforts across Federal Government

Supported GSA to publish updated Federal Website Standards

Established FASC working groups to evaluate sector-specific risks with drones and semiconductors

Issued M-24-15, *Modernizing FedRAMP,* to promote the use of secure cloud products and services

Established Chief AI Officer (CAIO) Council

Issued M-24-10, *Advancing Governance, Innovation, and Risk Management for Agency Use of AI*

Issued M-24-18, *Advancing the Responsible Acquisition of AI in Government*

21 TMF investments totaling $307.1 million

White House Roundtable on PQC

Expanded the AI training series across 3 tracks, engaging 14,000+ participants from nearly 200 government organizations

Managed and expanded AI Use Case Inventory

Issued joint ONCD-OMB guidance on cyber funding priorities for the Federal budget

Issued Annual FISMA Report

Published Federal Cybersecurity Progress Reports

CYBERSECURITY

Since Day 1, this Administration has been dedicated to strengthening America's cybersecurity, protecting our critical infrastructure, and improving the digital defenses of the Federal Government.

Following the 2020 SolarWinds cyber attack that allowed foreign adversaries to compromise the systems of thousands of SolarWinds customers, the President took decisive action in issuing EO 14028 on *Improving the Nation's Cybersecurity*. EO 14028 directed Federal agencies to strengthen their cybersecurity posture and adopt modern security practices such as zero trust (ZT).

Building on the direction of EO 14028, we pioneered a ZT strategy for the Federal Government through M-22-09, *Moving the U.S. Government Towards Zero Trust Cybersecurity Principles*. While continued effort is required to implement ZT, agencies have made tangible security gains to rapidly identify and eliminate malicious behavior before it can harm our national security. The cyber landscape is continuously evolving — and our adversaries are too — so we're working to secure Federal systems against all present and future threats as they become known to us.

We're helping agencies get on a sustainable path to implement the security practices highlighted in EO 14028.

WHAT	WHY	HOW
Securing Software	Cyber incidents like SolarWinds show the fragility of digital services when critical software is not secured.	M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*, and M-23-16, *Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*, outline steps for how agencies can use securely developed products. By acquiring and using products that are secure by design, agencies will protect critical software and software platforms from unauthorized access.
Deploying Multi-factor Authentication (MFA) and Encryption	We need to make our systems more defensible by consistently employing ZT principles to better detect and contain adversaries.	M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, directs agencies to invest in technology that is secure by design. Federal agencies responded to this call to action and developed ZT implementation plans, replacing ineffective deterrents like passwords with MFA. Agencies are also implementing higher levels of encryption, encrypting data in transit and data at rest.
Enhancing Investigative Capabilities	Logging information can provide "digital fingerprints" which can help us detect, investigate, and remediate cyber incidents.	M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, provides the first logging requirements for Federal agencies.
Enabling Continuous Monitoring	Despite our best efforts, cyber incidents do still occur. A continuously monitored, government-wide endpoint detection and response (EDR) system will help us better detect malicious cyber activity.	M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*, enables early detection, response, and remediation of cyber incidents via advanced technologies and leading practices.

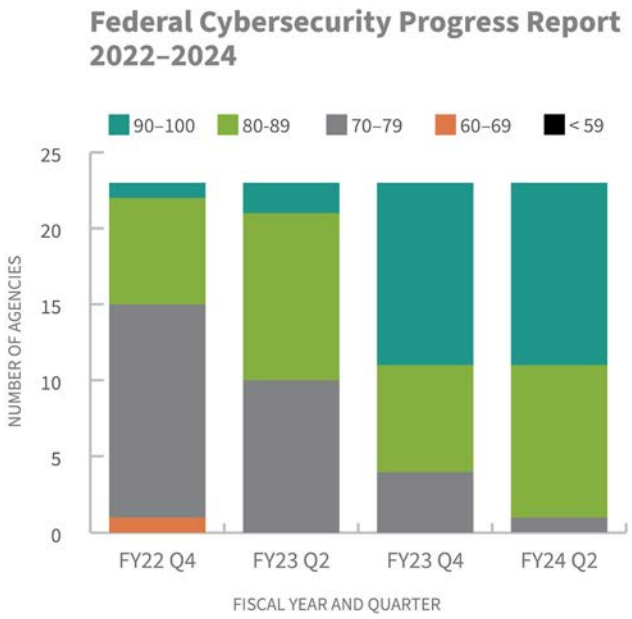
52% of Chief Financial Officers (CFO) Act Agencies have achieved more than 90% of EO 14028 milestones.

FISMA: Assessing the State of Federal Cybersecurity

Building on legal requirements adopted in 2002, the Federal Information Security Modernization Act of 2014 (FISMA) directs agencies to report on their information security programs to the Office of Management and Budget (OMB) and Inspectors General (IGs) to independently assess those programs. The categories of information reported as part of that process, called "FISMA metrics," provide a look into the state of Federal cybersecurity.

Since 2014, OMB has issued annual FISMA guidance and supplemental instructions for agency reporting called FISMA CIO Metrics. OMB uses the information reported by agencies to produce an annual FISMA report to Congress on the cybersecurity successes and challenges of the previous year.

As it oversees the paradigm shift for the security of agency networks, OMB is evolving how we measure progress. In 2022, we leveraged FISMA reporting to create the first Federal Cybersecurity Progress Report. This report, published twice per year, tracks agencies' progress in achieving EO 14028 milestones and implementing key cyber measures.



Launched in 2022, the Federal Cybersecurity Progress Report shows agency progress in achieving cybersecurity milestones. Agency scores are derived from FISMA metrics and aligned to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). This chart shows the total scores of the 23 CFO Act agencies assessed in this report, beginning in Fiscal Year (FY) 22 Quarter (Q) 4 through FY24 Q2.

Risk-based Guidance

OMB provides risk-based guidance to agencies, particularly when they're utilizing technology that could pose a threat to national security.

TikTok: We're directing agencies to remove applications that pose national security concerns. M-23-13, *"No TikTok on Government Devices" Implementation Guidance*, requires agencies to remove TikTok from Federal devices (except under specific circumstances).

Internet of Things (IoT)/Operational Technology (OT): We're helping agencies to better manage and secure their IoT and OT devices. M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*, requires agencies to begin inventorying their IoT and OT systems.

Unmanned Aircraft Systems (UAS)/Drones: We're guiding agencies in securely procuring and operating UAS, also known as drones. UAS are both aircraft and IT devices that can receive, collect, and transmit Federal data.

Cybersecurity — *continued*

The Quantum Race

Quantum computers hold the potential to drive innovations across the American economy. In addition to their many benefits, they pose serious risks, such as the possibility of breaking the encryption that protects our Nation's infrastructure and jeopardizing civilian and military communications.

Advanced quantum computers could pose a significant threat as early as 2030, which is why we've been working with agencies to become "quantum-resistant" before quantum computers become advanced enough to threaten our systems. To get there, we:

- Issued M-23-02, *Migrating to Post-Quantum Cryptography*, (PQC), which lays out steps for agencies to take as they prepare for migration to NIST cryptography standards.
- Released a report outlining a strategy and funding estimate for migrating systems to PQC while mitigating risks and harnessing benefits.
- Held a roundtable with cryptographers, industry, and agencies to discuss best practices for adopting PQC standards.

Migration to PQC may involve over 4,000 agency systems, at a projected cost of $7.1 billion.[1] This effort will take sustained government-wide collaboration and investments across multiple years. Looking ahead, under National Security Memorandum 10 (NSM-10), OMB will assist agencies as they:

- Prioritize the transition of public networks and systems to quantum-resistant cryptography-based environments.
- Develop complementary mitigation strategies to provide cryptographic agility in the face of unknown future risks.

1 This is an estimate as not all systems may be migrated to PQC. For example, some systems may be retired or exempt.

Resourcing Critical Cyber Investments

We work with agencies to allocate cyber funding, ensuring the Government is resourced to strengthen our Nation's cyber defenses.

Over the past 2 years, the Administration increased the focus and spending on cybersecurity priorities from $9.9 billion in FY22 to nearly $13 billion proposed in the President's Budget for FY25, a 16% increase over 2 years.

Securing the Federal IT Supply Chain

Established by the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure (SECURE) Technology Act, the Federal Acquisition Security Council (FASC) is responsible for coordinating a whole-of-government approach to identify and address risks to the Federal Government's information and communications technology (ICT) supply chain.

Over the past 4 years, OFCIO chaired the FASC, convening senior leaders across 12 agencies and maturing the Council to establish processes for interagency evaluation of significant supply chain risks. Despite having no appropriated resources, the FASC began execution on its supply chain risk management policy and operational responsibilities, putting in place a critical framework for future administrations to build upon.

Cybersecurity is a Team Sport

We work closely with our partners at the Office of the National Cyber Director (ONCD) and the Cybersecurity and Infrastructure Security Agency (CISA) to drive coordinated cybersecurity action across Government. ONCD sets the national cyber–security strategy, CISA leads operational efforts and incident response, and OMB ensures the Federal budget and policy align with cybersecurity priorities. Together, these agencies form a cybersecurity trifecta of governance and execution.

Partnership in Action

Recognizing the need for investment prioritization and alignment, the Administration provides joint OMB-ONCD guidance on cybersecurity funding priorities for the Federal budget. Published for the first time in 2022, this guidance ensures agency cybersecurity spending aligns with Administration priorities and the National Cybersecurity Strategy (NCS).

(Above) Federal CIO Clare Martorana and CISA Director Jen Easterly speak on an opening panel, moderated by Siobhan Benita with *Global Government Forum*, at GovernmentDX 2024. (Below) Federal CIO Clare Martorana and National Cyber Director Harry Coker speak on a closing panel at GovernmentDX 2024.

Collaboration Between Federal IT and Security Leaders. In support of Cybersecurity Awareness Month and with its theme "Secure Our World," Federal CIO Clare Martorana and Acting Federal Chief Information Security Officer (CISO) Michael Duffy convened a joint in-person meeting of the CIO and CISO Councils. Agency leaders in IT and cybersecurity gathered for a group photo in October 2024 at the Eisenhower Executive Office Building after discussions on FY25 IT and cybersecurity priorities.

TECHNOLOGY MODERNIZATION AND DATA

Technology and data power agencies to deliver on their missions. The faster we can adopt modern technologies and strengthen data integrity, the faster we can deliver trusted services for the American public.

The American public and Federal agencies alike benefit from the continued modernization of technology.

Modernization improves the efficiency and effectiveness of Government operations, lowering administrative burden for the workforce, enabling agencies to better fulfill their missions, and streamlining service delivery to the public.

Our actions are driven by three principles: Accelerate, Align, Unlock.

- **Accelerate capability delivery and strategy** to enable greater, faster technical delivery to better serve the mission.
- **Align resources and performance** to drive greater return on investment (ROI) in IT investments and align resources to IT lifecycles and needs.
- **Unlock information and data management** to improve decision-making, data access, and transparency.

By building this enterprise technology framework, we're enabling agencies to: make quick and efficient decisions informed by data; seamlessly communicate within the Federal Government and between state, local, tribal, and territorial (SLTT) governments; proactively and securely meet the needs of the public; and maintain agility to adapt to emerging circumstances, like severe weather events, health emergencies, or malicious cyber attacks.

FedRAMP: Accelerating Cloud Adoption

We're making it easier and faster for agencies to use modern cloud technology that improves innovation, provides better reliability for the public, increases performance and efficiency, and helps to lower IT costs.

First established in 2011, the Federal Risk and Authorization Management Program (FedRAMP) helps agencies safely accelerate their adoption of cloud computing products and services by offering a consistent and reusable authorization process. FedRAMP empowers agencies to use modern cloud technologies, with an emphasis on security and protection of Federal information. In December 2022, the FedRAMP Authorization Act was signed as part of the National Defense Authorization Act (NDAA) for FY23. The NDAA codifies FedRAMP as the authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified Federal information.

In July 2024, we issued M-24-15, *Modernizing the Federal Risk and Authorization Management Program (FedRAMP)*, to significantly bolster FedRAMP's role as a **cornerstone of Federal cloud security.** It defines a broad reach for FedRAMP, establishes a new governance structure, and improves the authorization process for secure cloud adoption.

Throughout 2024, we conducted more than 20 agency roadshows to share guidance highlights, hear agency plans to scale FedRAMP usage (e.g., presumption of adequacy; reuse; Governance, Risk, and Compliance [GRC] tools), and determine how OMB can best support agency implementation of the guidance.

FITARA: Federal Information Technology Acquisition Reform Act

Progress in IT modernization requires collaboration between agency CIOs, OMB, and Congress to align policy, law, and funding to common goals. The Federal Information Technology Acquisition Reform Act (FITARA) Scorecard is an example of Congress's commitment to overseeing agency progress. During this Administration, ***agencies increased their scores one full letter grade*** — from a B to A in overall grade average and from a C to B in cyber.

Zero Trust Data Security

Data is foundational to effective zero trust (ZT) implementation, and we're building bridges between data and security teams across Government to better secure our data and systems from adversaries.

The Federal ZT Strategy (M-22-09) charged the Federal Chief Data Officer (CDO) Council and Federal CISO Council to convene a cross-agency working group of data and security experts to develop a Federal data security guide. More than 30 Federal agencies answered the call to author the Guide, a first-of-its-kind document that will help practitioners operationalize data security using a ZT framework.

Open Data

Federal data is a valuable national resource and a strategic asset. Expanding the accessibility and usability of such data promotes transparency and trust, increases community engagement, accelerates opportunities to leverage AI, and informs evidence-based and data-driven decision-making.

The scale of Government data has increased exponentially since we first launched our open data policy in 2013, so we're working to strengthen the Government's use and administration of data. This includes delivering on open data and data inventory requirements under the Open, Public, Electronic, and Necessary Government Data Act of 2019, such as expanding data.gov data sets. We're also facilitating the adoption of open data practices across Government by partnering with the General Services Administration (GSA) and the National Archives and Records Administration to develop and maintain open data tools and resources like the Federal Data Catalog and resources.data.gov.

Technology Modernization Fund: Innovative Funding Model

The Technology Modernization Fund (TMF) is an innovative investment program transforming how agencies deliver simple, seamless, and secure services to the public.

To date, the TMF has allocated over $1 billion for 69 investments across 34 Federal agencies. Over 90% of that funding was invested during this Administration to deliver a Government that meets today's expectations. See pg. 12 for a *Spotlight on the TMF.*

The TMF is on its way to becoming the funding vehicle of choice for agencies who need to accelerate legacy IT modernization, enhance cybersecurity, improve digital service delivery, promote cross-agency collaboration, and increase ROI.

Why TMF?

Incremental Funding: Iterative funding, tied to delivery of milestones, enables dynamic implementation and ensures responsible use of taxpayer dollars.

Our Board: The interdisciplinary executive-level TMF Board rigorously evaluates and interrogates projects and positions them for success.

Technical Expertise: Project teams can leverage experts in design, engineering, acquisition, and more.

Lessons Learned: We surface lessons learned, share solutions and best practices, and help agencies connect and learn from one another.

TECHNOLOGY MODERNIZATION AND DATA — *continued*

88% of TMF investments help bolster the Nation's cybersecurity

Spotlight on the TMF

Since its creation in 2018, the TMF has undergone significant evolution, increasing its annual investment rate by more than 18 times, from $20 million in 2018 to $362 million in 2021 — the first year of this Administration. This evolution was made possible by Congress's historic infusion of American Rescue Plan (ARP) funds for the TMF to support pandemic response and address urgent IT modernization challenges. Fifty-two of the TMF's 69 investments were made with ARP funds.

34 AGENCIES

$1B+ INVESTED

69 PROJECTS

Projected Impact of TMF Investments Made During this Administration

52% *will save Government labor hours*

58% *will support interagency collaboration*

21% *will support underserved communities*

40% *will reduce burden hours for the public when accessing Federal services*

Hear How the TMF is Making a Difference at Agencies

"By modernizing our school websites and updating school branding, we are improving how our schools communicate with students, parents, and communities."

Tony L. Dearman, Director, Bureau of Indian Education (Department of the Interior)

"The TMF funds are the essential lifeblood allowing the Office of Workers' Compensation Programs (OWCP) to modernize critical claims adjudication and payment systems that are beyond end of life and over 20 years old."

Douglas Pennington, Deputy Director for Operations & Finance, OWCP (Department of Labor)

"The TMF has advanced cybersecurity in a few years what would have taken a decade. We have implemented several levels of maturity in [Zero Trust] capability and program maturity through the investment…and accelerated the Department's cybersecurity program to both be measured as "effective" by our Inspector General, and also measured as an "A" through the FITARA reporting Process."

Steven Hernandez, CISO (Department of Education)

TMF investments are helping people by...

 Improving public health and safety around nuclear and radiological threats by modernizing applications and streamlining decision-making in response to nuclear emergencies. **Department of Energy**	 Helping weather forecasters and their partners in over 150 National Weather Service offices worldwide deliver life-saving forecasts and warnings by modernizing Weather.gov. **Department of Commerce**	 Helping over 153 million workers, retirees, and their families access the benefits they've earned via a "Lost and Found" registry to search for unclaimed, lost, or forgotten retirement savings and benefits. **Department of Labor**
 Improving service and consumer protection for air travelers by streamlining the complaint process, protecting consumer data, and using intuitive tools for the aviation industry. **Department of Transportation**	 Improving the digital experience for over 43 million student loan borrowers by centralizing and merging loan information on StudentAid.gov. **Department of Education**	 Helping create employment opportunities for more than 36,000 individuals who are blind or have disabilities by modernizing the AbilityOne Commission's systems. **AbilityOne Commission**
 Reducing wait times for over 70 million Americans who depend on Social Security services by accelerating the transition to e-signatures and an online document platform. **Social Security Administration**	 Protecting journalists and their sources stationed in high-risk areas around the world by safeguarding the integrity of the U.S. Agency for Global Media's (USAGM) news content. **USAGM**	 Developing a unified, modern way for veterans to access benefits by digitizing forms across the Department of Veterans Affairs (VA) and personalizing experiences. **VA**
 Improving communication and access to education services for Tribal communities and schools by accelerating website modernization for up to 183 Bureau of Indian Education-funded schools. **Department of the Interior**	 Increasing diplomacy for over 270 State Department diplomatic posts worldwide by harnessing safe, secure, and responsible generative AI to empower its widely dispersed team members to work more efficiently. **Department of State**	 Accelerating cybersecurity updates at the National Aeronautics and Space Administration (NASA) to support their mission, from controlling spacecraft to enabling secure collaboration with international space agencies and researchers worldwide. **NASA**

"The TMF investment will enable the National Weather Service (NWS) to move its web services into the 21st century, [providing] information that every member of the public can understand and use at a moment's notice to stay safe."

George Jungbluth, Director of NWS Office of Dissemination (Department of Commerce)

"USAID's investment from the TMF enabled us to launch the Agency-wide CRM system, COMPASS, nine months ahead of schedule… [providing] USAID end users with the necessary tools of a modern platform to manage strategic relationships and engagements more effectively and efficiently."

Jason Gray, CIO (U.S. Agency for International Development)

DIGITAL SERVICE DELIVERY

Each year, the Federal Government delivers services to more than 330 million people. We're building a strong foundation to provide exceptional digital and customer experiences to the American public.

The 21st Century Integrated Digital Experience Act (21st Century IDEA), a bipartisan act signed into law in 2018, calls on agencies to modernize their websites and improve digital service delivery. Building on the law, EO 14058 on *Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government* laid the framework for delivering a digital-first customer experience (CX).

Since then, we've maintained momentum by standing up a digital experience team dedicated to digital service delivery, prioritizing CX on the President's Management Agenda, and integrating digital experience into Federal policies and standards:

1. **M-23-10,** *The Registration and Use of .gov Domains in the Federal Government*, is a foundational step to ensure public trust in digital interactions.
2. **M-23-22,** *Delivering a Digital-First Public Experience*, sets the vision and requirements for a 21st century digital experience.
3. **M-24-08,** *Strengthening Digital Accessibility and the Management of Section 508 of the Rehabilitation Act*, guides agencies in making their IT more broadly accessible.
4. **Federal Website Standards** help agencies provide high-quality, consistent digital experiences for everyone.

Together, this policy framework calls for agencies to modernize websites and digital services, digitize forms and services, ensure accessible digital experiences, and fully leverage centralized shared services.

The Digital Landscape: Digital is Now the Default

The Federal Government is an enormous service provider, with agencies delivering information and services to more than 330 million people.

Digital is now the default way the public interacts with the Government — and they expect their online experiences to be consistent with their favorite consumer websites and mobile apps. More than ever, digital experience is central to Federal agencies' mission delivery and our Government's ability to serve the American people.

80M
hours spent accessing Federal websites each month

1.7B
visits to Federal websites each month

A Foundation for Delivery: We Now have Better...

Visibility

into the Federal Government's vast website and digital service ecosystem through the inventory required under M-23-22.

Leadership and Accountability

through agency designation of digital delivery leads and Section 508 program managers.

Measurement of Progress

through expanded automated scanning of website performance indicators and the Section 508 annual assessment.

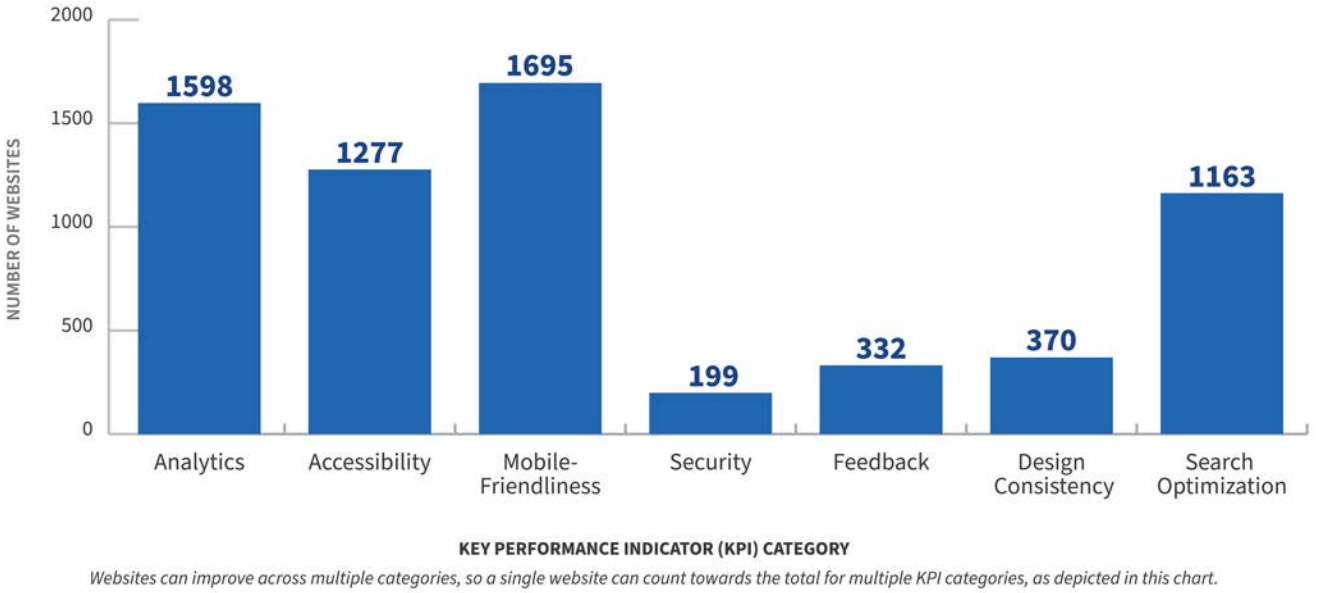
Cross-agency Coordination

through the Digital Experience Council, a new subcommittee of the CIO Council that partners with agency practitioners to deliver a digital-first public experience.

Delivering Impact at Scale

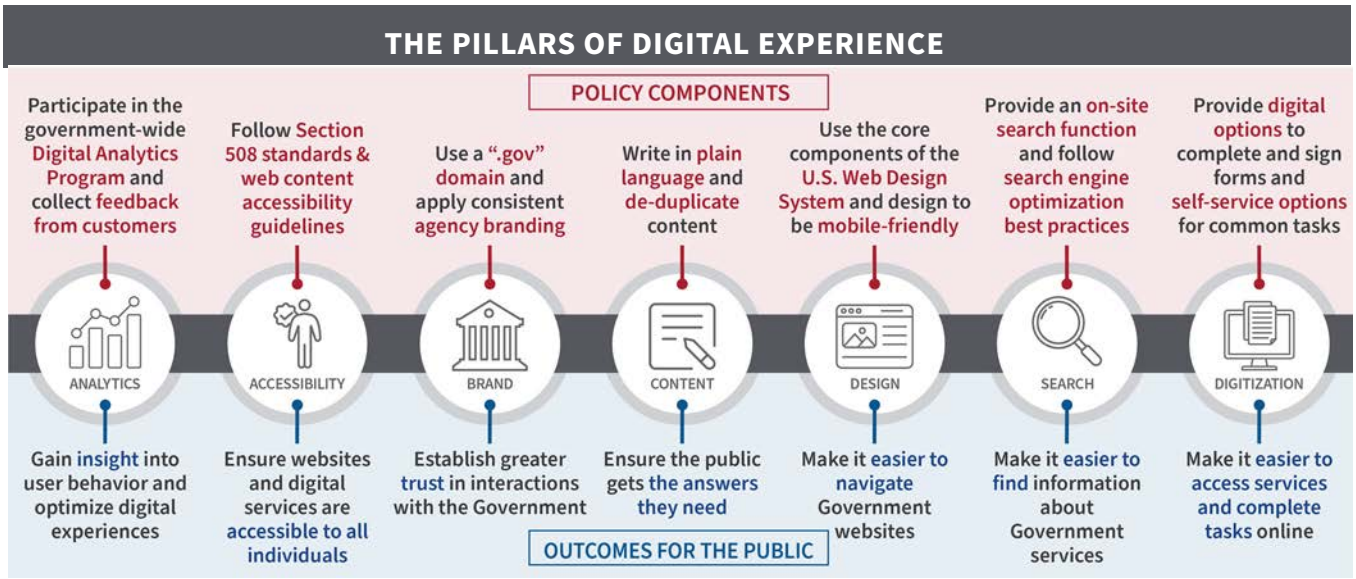
With the policy framework and shared tools in place to deliver better digital experiences to the American public, agencies are making tangible progress.

More than 3,500 Federal Government websites have improved within the last year.



Websites can improve across multiple categories, so a single website can count towards the total for multiple KPI categories, as depicted in this chart.

DIGITAL SERVICE DELIVERY — *continued*



Delivering Where it Matters Most

Agencies have delivered big wins for the American public that exemplify the continued progress across the Federal enterprise. Some include:

CDC

The Centers for Disease Control and Prevention (CDC) streamlined content and ensured accessibility on CDC.gov, archiving more than 65% of outdated or inaccessible materials and rewriting key content to best meet user needs.

CMS

The Centers for Medicare & Medicaid Services (CMS) updated Medicare.gov to highlight the tasks and information most frequently sought by users, including a redesigned Medicare Plan Finder.

FEMA

The Federal Emergency Management Agency (FEMA) redesigned the FEMA.gov homepage to provide information that helps users know their risk, be more prepared for a disaster, and jumpstart their recovery after disasters strikes.

IRS

The Internal Revenue Service (IRS) improved online content for first-time taxpayers so they could find the information they needed this tax filing season. Within the first month, this content had over 100 million views, nearly 30% of all traffic to IRS.gov.

SSA

The Social Security Administration (SSA) redesigned SSA.gov with content written in easy-to-understand language in both English and Spanish.

VA

The Department of Veterans Affairs (VA) continued to serve its users digitally through its Health and Benefits mobile app. A recent update enabled blind Veterans to read their VA benefits decision letters inside the app using assistive technology.

ARTIFICIAL INTELLIGENCE

We established an expert AI team to support AI adoption and engagement across the Federal Government, and to prepare for and accelerate future technological advancements.

The Government must keep pace with new technologies as they emerge, and we saw this unfold in real time with the explosion of AI tools, such as ChatGPT, seemingly overnight. We were ready, and deployed a first-of-its-kind Federal AI policy framework.

In 2023, the President issued EO 14110 on *the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, the most significant action any government in the world has ever taken on AI.

As the United States takes action to realize the tremendous promise of AI while managing its risks, the Federal Government will lead by example and provide a model for the responsible use of AI. As part of this commitment, OMB delivered on a major EO milestone with the issuance of M-24-10, *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence* — OMB's **first binding guidance on AI** governance, innovation, and risk management. The policy sets our values clearly: it puts people and communities at the center of the Government's innovation goals, while empowering agencies to responsibly leverage AI to advance their missions.

To ensure that agencies can deliver on these policies, we made **groundbreaking investments in AI**, including $30 billion for Federal use of AI. Of that $30 billion, $70 million is for M-24-10 implementation, and $32 million is for building Federal AI talent. Collectively, these actions are putting the United States on the path to lead the way in responsible AI innovation.

In March 2024, agency Chief AI Officers (CAIOs) attended a CAIO Council meeting held at The White House to discuss the issuance and forthcoming implementation of M-24-10, OMB's first ever government-wide policy to strengthen governance, advance innovation, and mitigate risks of AI.

> *Agencies have completed on schedule each action that EO 14110 tasked for 2024—more than 100 in all.*

ARTIFICIAL INTELLIGENCE — *continued*

By implementing M-24-10, we are:

1. **Strengthening AI Governance**
   We defined roles and responsibilities for newly designated CAIOs to promote AI innovation and manage risks from AI, in collaboration with other agency officials.

2. **Advancing Responsible AI Innovation**
   We directed agencies to develop enterprise AI strategies and provided recommendations on removing barriers to responsible innovation.

3. **Managing Risks from the Use of AI**
   We prioritized agency AI risk management resources towards higher-risk use cases and mandated minimum risk management practices to protect the safety and rights of Americans.

Coordinating AI Across Government

We launched the CAIO Council to coordinate the development and management of AI across Government. Agencies have designated a CAIO as their accountable agency leader responsible for AI governance, and particularly for managing agency uses of AI that impact the rights and safety of the public. The new CAIO Council, chaired by the Federal CIO, ensures coordination, harmonization, and accountability as agencies implement EO 14110 and corresponding guidance.

Sharing How the Federal Government Uses AI

The Government is using AI to better serve the public, with over 700 use cases reported in healthcare, transportation, and other fields. First required under EO 13960 on *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government* and later codified by the Advancing American AI Act, the annual AI Use Case Inventory provides the public with necessary transparency into the ways Federal agencies use AI.

We've made significant improvements to the Inventory, including: (1) transitioning to a data collection platform that allows for increased data validation and data quality checks and (2) expanding what agencies are required to report on in their inventories in response to M-24-10. These new collection methods will promote data integrity and transparency, as well as improved reporting on budgetary impacts for AI adoption.

The AI Use Case Inventory also provides an opportunity for agencies to identify areas for collaboration, as it illustrates where similar use cases are being explored across agencies. These interagency harmonization efforts are further evaluated through the CAIO Council.

Empowering Agencies to Responsibly Acquire AI

As the largest single consumer in the United States economy, the Government's procurement decisions have far-reaching implications. M-24-18, *Advancing the Responsible Acquisition of Artificial Intelligence in Government*, serves as a first step to catalyze innovation throughout the Federal Government by ensuring that agencies and vendors grow together as the AI market continues to evolve — charting the course for ensuring that Federal acquisition of AI enables agencies to responsibly optimize delivery of their missions for the American people.

Strengthening Government Content Authentication

The public needs to be able to trust the digital services that the Government provides, so we're working on ways that the public can independently verify whether content was published by the Government. In partnership with NIST, we'll share best practices for content authentication, guaranteeing the integrity of agency online content.

Training the Federal Workforce in AI

As AI becomes increasingly prevalent in society and used in Government operations, we must ensure we have the right team in place to support responsible implementation. In 2023, we launched the first series of AI Trainings for the Federal Workforce, in collaboration with GSA's Centers of Excellence and the Stanford University Institute for Human-Centered AI (HAI). This training fulfills the mandates included in the AI Training Act and EO 13960 on *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government.*

This year, we expanded the AI training series, tripling the number of sessions across three tracks — each taught by different academic partners, including the George Washington University Law School, the Stanford University Institute for HAI, and the Princeton Center for IT Policy:

i. **Acquisitions:** Equipping Federal employees with tools and knowledge about effectively procuring and managing the use of AI technologies.
ii. **Leadership and Policy:** Empowering Federal leaders with the insights and strategies necessary to carefully guide responsible AI initiatives and adoption within their agencies.
iii. **Technical:** Bolstering Federal employees' technical understanding for developing, deploying, and governing AI technologies.

Snapshot: 2024 AI Training Series

92%
average participant satisfaction rating

190+
unique Government organizations represented

14,000+
participants registered

95%
increase in registration from inaugural training series offered in 2023

Agencies have reported 700+ use cases for AI across Government, including:

Analyzing Weather Hazards — The National Oceanic and Atmospheric Administration (NOAA) uses AI to provide notifications to keep people safe from severe weather events.

Proactive Health Services Resourcing — The Department of Health and Human Services uses AI to predict and mitigate infectious diseases, prescription drug shortages, and supply chain issues.

Improving Response to Natural Disasters — FEMA uses AI to quickly review and assess structural damage in the aftermath of hurricanes, and NOAA is developing AI to conduct more accurate forecasting of extreme weather, flooding, and wildfires.

Capturing Actionable Feedback from Veterans — VA uses AI to organize feedback from veterans on their experience interacting with the VA. AI helps sort free-text comments by topic area, capture major trends, and facilitate processing and effective case management.

Protecting Public Safety — The Federal Aviation Administration uses AI to help deconflict air traffic in major metropolitan areas to improve travel time, and the Federal Railroad Administration is researching AI to help predict unsafe railroad track conditions.

Optimizing Patent Evaluation — The U.S. Patent and Trademark Office uses AI to help examiners locate relevant documents and compare patent applications with existing works, streamlining the patent adjudication process.

POWER OF PARTNERSHIPS

Imagine a day when a member of the American public can use their mobile phone to access everything they have in flight with the Federal Government — a small business loan application, the status of a tax refund, or their estimated Social Security retirement benefits. The process is easy, convenient, secure, fast, and works for people of all abilities — just like the consumer experiences we have every day outside of government, from online banking to ordering food delivery. This is not only possible — the Biden–Harris Administration has been helping to make it happen.

"Modernizing Government technology is a marathon, not a sprint, and millions are counting on the next leg of the race to be even stronger. As I pass the baton to a new team, I do it with great admiration for the many partners and technologists who gave it their all over the past four years, and with great confidence that the next team will run even faster in delivering the Government we all know is possible."

— Clare Martorana, Federal CIO

Through the power of partnerships, we have put the policies in place to deliver the simple, seamless, and secure digital experience the American people deserve when interacting with the Government.

This is just the beginning, and future Federal CIOs should leverage and continue to build these partnerships to further accelerate progress and deliver impact with taxpayer dollars.

In April 2024, OMB welcomed international digital government leaders to The White House for a day of discussions on bolstering cybersecurity, modernizing technology, and delivering Government digital services that meet today's expectations. Leaders attended from Azerbaijan, Canada, Germany, Iceland, Netherlands, Singapore, Trinidad and Tobago, United Kingdom, and the United Nations.

Strengthening Partnerships Across Government to Deliver Better Results

- **Executive Office of the President (EOP):** OMB, as part of the EOP, is uniquely positioned to have a birds-eye view of the Federal landscape and partners with other EOP components — including ONCD, the Office of Science and Technology Policy, the National Security Council, and others — to manage government-wide tech initiatives.
- **Management + Budget:** OFCIO Desk Officers (DOs) partner with Program Examiners to interrogate agency IT budget requests, ensuring the right investments are made at the right time. DOs also help agencies navigate challenges to accelerate digital modernization.
- **Engine of Digital Delivery:** OMB's OFCIO and U.S. Digital Service (USDS) partner with GSA to set policies, create shared solutions, and encourage best practices to empower agencies to invest in the best IT tools and services.
- **Defending Federal Systems:** EO 14028 set Federal civilian agencies on the pathway to zero trust (ZT) and OMB has followed through with further guidance and support as agencies make that journey. OMB also works to coordinate civilian ZT efforts with those in the Department of Defense, the Intelligence Community, CISA, and other cyber partners.
- **Senior Leaders and Technology Teams:** Protecting and modernizing the systems and data we manage on behalf of the American people is not solely a CIO's job; it takes cross-cutting leadership to make strategic investments and deliver digital transformation.
- **Executive Councils:** Interagency forums like the CIO Council, CISO Council, CAIO Council, and Digital Experience Council are key to driving progress towards an Administration's goals.

The engine of modern Government service delivery: Technology powers the Federal Government's ability to deliver on its mission — and OFCIO, USDS, and GSA work in lock step to accelerate digital modernization. OFCIO sets the tech policy, USDS delivers the products and solutions, and GSA provides the shared services and standards agencies need to move faster. Meet the leaders of these Federal tech teams: (L to R) USDS Administrator Mina Hsiang, GSA Administrator Robin Carnahan, and Federal CIO Clare Martorana.

> *"Thanks to the Biden-Harris Administration's commitment to customer experience and digital delivery, today we're closer than ever before to a future where interacting with the Government online is as seamless and secure as the other online transactions in our daily lives. We see that in strategic partnerships with OFCIO and USDS, our tech policy and delivery teams, to launch policies that meet today's needs, surge tech talent to deliver products and services that meet today's expectations, and leverage GSA's shared services and solutions like Login.gov, IRS Direct File, and Notify.gov to directly serve the American people. We see it in the innovative IT contracts, changes that strengthen FedRAMP and make it easier for technology companies to do business with Government, and in the Technology Modernization Fund and other agile IT procurement initiatives that ensure taxpayers get the best value for their money. In these ways, and so many more, GSA has been proud to contribute to this Administration's historic record of helping Government deliver what the American people need, when they need it."*
>
> **—Robin Carnahan, Administrator, GSA**

Building National and International Partnerships to Improve U.S. Readiness

- **Global:** As called for in the National Cybersecurity Strategy, the Government is "[forging] international partnerships to pursue shared goals." In 2024, OFCIO convened global leaders from 10 countries at The White House for a day of discussions on delivering an accessible secure digital Government experience to the public. Key relationships between U.S. and international government partners were built and will continue into the next administration.
- **Whole-of-Society:** Addressing cyber threats requires a whole-of-society approach across Federal and SLTT governments, Congress, the private sector, nonprofits, and academia.

Successful Baton Passes Are Crucial to Maintaining Momentum and Driving Progress

To pass the baton of progress forward, agencies must build bridges with our partners. Widespread collaboration and sharing of lessons learned — across Government, industry, and the globe — can empower CIOs with the tools and information they need to secure, modernize, and leverage technology across their agencies and departments. While agencies have built a foundation of readiness over the past several years, sustained progress relies on creating resilient formations — strong career teams, industry partnerships, and interagency collaborations that can maintain momentum through administration changes.

At the end of the day, the Government's success is not measured by what any single team or administration accomplishes alone, but by how effectively it is meeting the needs of the millions of people it serves. While there's more to be done, OMB and agencies have made great strides and are committed to delivering the Federal Government the American public deserves.

Join us.

OFCIO has achieved a great deal over the past several years, and the work will continue. We need technologists at the table collaborating with our Nation's leaders. To learn more about serving our country, visit cio.gov/entry-to-the-government.

"Our Nation's security requires strong collaboration across the Federal cybersecurity ecosystem and we are proud of the partnership and work we have accomplished with OMB over the past three years. ONCD and OMB have successfully demonstrated this partnership through our annual joint cybersecurity priorities memo giving important budget guidance to our interagency partners, and we have worked to ensure the Federal CISO is a dual-hat role between our organizations ultimately ensuring a more streamlined, harmonized, and effective approach to Federal cybersecurity. We look forward to continuing the strong relationships we've developed to continue to advance Federal cybersecurity and IT modernization in the months and years ahead."

— Harry Coker, National Cyber Director, ONCD

"Securing Federal networks and protecting the data and information the Government relies on requires a coordinated, team effort. CISA is proud to be part of a team that has accomplished so much over the last four years. As the operational lead for Federal cybersecurity, CISA has provided a common baseline of security across the Federal civilian executive branch and helped the Federal Government achieve an unprecedented level of visibility into its real-time cybersecurity posture, including what types of hardware and software we are running, and whether they're protected against known vulnerabilities. While our list of accomplishments is long, work remains to be done. CISA will continue working with our Federal Government partners to modernize cybersecurity and guard against threats to Federal systems and networks."

— Jen Easterly, Director, CISA

RESOURCES

Executive Orders

Executive Order 14028 on *Improving the Nation's Cybersecurity* (May 12, 2021)

Executive Order 14058 on *Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government* (December 13, 2021)

Executive Order 14110 on *the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (October 30, 2023)

OMB Memoranda

M-21-30, *Protecting Critical Software Through Enhanced Security Measures* (August 10, 2021)

M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (August 27, 2021)

M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response* (October 8, 2021)

M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements* (December 6, 2021)

M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (January 26, 2022)

M-22-16, *Administration Cybersecurity Priorities for the FY 2024 Budget* (July 22, 2022)

M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (September 14, 2022)

M-23-02, *Migrating to Post-Quantum Cryptography* (November 18, 2022)

M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements* (December 2, 2022)

M-23-10, *The Registration and Use of .gov Domains in the Federal Government* (February 8, 2023)

M-23-13, *"No TikTok on Government Devices" Implementation Guidance* (February 27, 2023)

M-23-16, *Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (June 9, 2023)

M-23-18, *Administration Cybersecurity Priorities for the FY 2025 Budget* (June 27, 2023)

M-23-22, *Delivering a Digital-First Public Experience* (September 22, 2023)

M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements* (December 4, 2023)

M-24-08, *Strengthening Digital Accessibility and the Management of Section 508 of the Rehabilitation Act (digital)* (December 21, 2023)

M-24-10, *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence* (March 28, 2024)

M-24-14, *Administration Cybersecurity Priorities for the FY 2026 Budget* (July 10, 2024)

M-24-15, *Modernizing the Federal Risk and Authorization Management Program (FedRAMP)* (July 25, 2024)

M-24-18, *Advancing the Responsible Acquisition of Artificial Intelligence in Government* (October 3, 2024)

Press Releases

Preparing to Welcome the 2022 U.S. Digital Corps (June 10, 2022)

Celebrating 5 Years of the Technology Modernization Fund (March 14, 2023)

Readout of White House Multifactor Authentication Modernization Symposium (July 18, 2023)

FACT SHEET: OMB Releases FedRAMP Guidance to Accelerate the Secure Adoption of Cloud Services (July 26, 2024)

FACT SHEET: Building Digital Experiences for the American People (September 22, 2023)

Why the American People Deserve a Digital Government (September 22, 2023)

Readout of White House Roundtable on Protecting Our Nation's Data and Networks from Future Cybersecurity Threats (February 12, 2024)

Progress Towards Delivering a Digital-First Public Experience (April 17, 2024)

Readout of White House Meeting Convening Global Leaders on Delivering a Secure Digital Government Experience (April 19, 2024)

FACT SHEET: Biden–Harris Administration Continues Work to Secure a Post-Quantum Cryptography Future (August 13, 2024)

RESOURCES *— continued*

Other

The Call to Serve: Help Us Tackle the Nation's Tech Challenges

Requirements for Delivering a Digital-First Public Experience

Federal Website Standards

Reports

FY20 FISMA Report to Congress (May 21, 2021)

FY21 FISMA Report to Congress (September 14, 2022)

FY22 FISMA Report to Congress (May 1, 2023)

FY23 FISMA Report to Congress (June 7, 2024)

Report on Post-Quantum Cryptography (July 29, 2024)

Strategies and Guides

Federal Information Technology Operating Plan (June 2022)

Federal Zero Trust Data Security Guide (October 2024)

Websites

AI.gov

cio.gov

data.gov

digital.gov

IT Dashboard

performance.gov/cyber

tmf.cio.gov

whitehouse.gov/omb/management/ofcio

OFCIO

OFFICE OF THE FEDERAL
CHIEF INFORMATION OFFICER