Modernize IT to Increase Productivity and Security

Goal Leaders

Steve Censky, Deputy Secretary, United States Department of Agriculture

Maria Roat, Deputy Federal Chief Information Officer, Office of Management and Budget

September 2020

Goal Statement

- The Executive Branch will build and maintain more modern, secure, and resilient information technology (IT) to enhance mission delivery and productivity – driving value by increasing efficiencies of Government IT spending while potentially reducing costs, increasing efficiencies, and enhancing citizen engagement and satisfaction with the services we provide.

Challenges

- Limited accountability for achieving enterprise-wide outcomes that enhance IT service effectiveness and reduce cybersecurity risks.
- Slow adoption of cutting-edge commercial technologies due to onerous acquisition and authorization processes.
- Federal agencies employ patchwork network architectures and rely on legacy systems that are costly and difficult to secure and upgrade.

Opportunities

- Expand the use of modern commercial technologies that are effective, economical, and secure.
- Reduce the impact of cybersecurity risks by safeguarding IT systems, sensitive data, and networks.
- Leverage common solutions and innovative practices to improve efficiency, increase security, and ultimately meet citizens' needs.

The Federal Government has made significant progress in meeting its IT Modernization agenda:

Updating Policies

OMB has removed barriers to rapid adoption of best-in-class commercial solutions to better meet the needs of citizens through updated policies and strategic directives.

- Modernizing Government Technology Act
- Trusted Internet Connections
- High Value Assets
- Identity Credential and Access Management
- Cloud Smart
- Data Center Optimization Initiative
- Federal Acquisition Supply Chain (FASC)

Building Cyber Capacity

Agencies have made substantial progress to protect the data of the public. Of the 23 Civilian CFO Act agencies:

- **Mobile Device Management** – 22 agencies are able to remotely wipe contents of lost or stolen mobile devices.
- **Automated Access Management** – 19 agencies have central and dynamic control and monitoring of users' access.
- **Exfiltration and Enhanced Defenses** – All 23 agencies met targets for email and traffic filtering.
- **Cloud Email** - 84% of agency inboxes are hosted on cloud email servers. All 23 Agencies have made progress and have a plan to complete.

Investing in Modernization

The **Technology Modernization Fund** (TMF) board was established, funding 9 projects totaling $90 million dollars, including:

- Farmers.gov, a single web portal for services for farmers.
- Acceleration of the Federal-wide shared service for payroll (NewPay).
- Modernization of foreign labor certification within the Visa application process.
- Modernization of decades-old, custom legacy applications at HUD.
- Acceleration of Cloud email at Department of Energy to migrate over 40 systems to a single common platform.

The Federal Government has made significant progress addressing workforce challenges of IT community:

Reskill

Federal CIO community has invested in pilot programs to build IT skills of people inside and outside the IT community.

- **Federal Cybersecurity Reskilling Academy** launched in November 2018. Two cohorts were run targeting people from both inside and outside IT. Lessons learned from these initiatives will shape future programs.
- **Robotic Process Automation** training was offered to targeted Agency individuals to build automation skills.
- **Communities of practice** for key skills-AI, RPA, and Cloud
- **Data Science** reskilling is planned for 2020.

Recruit

We are modernizing our recruitment of top-tier candidates through improved hiring processes and more competitive pay.

- **Code challenges** styled after private sector recruiting to attract competitive applicants and benchmark their skills.
- **Implementing market-informed compensation** to make Federal IT jobs more competitive at every level.
- **CIO visits** with students at schools with Data, Cyber and AI programs.
- **Sharpening recruiting tactics:** hiring events at major talent hubs; data-driven workforce planning; and updated, modern, flexible PDs to attract top talent.
- **CIO initiatives** to develop community leadership.

Retain

Making the Federal Government a premier employer of IT talent at entry, mid-career, and senior levels.

- **Greater mobility** among IT jobs within the Federal government.
- **Experiential learning** including expanded, targeted developmental details (cyber, supply chain, data science), fellowships, and cross-sector experiences.
- **Training** to provide foundational knowledge for professionals to expand their skills, and apply this learning to delivering mission value.
- Focus on **developing diverse leadership** through programs like Women in IT, CIO Council project opportunities, and workgroup leadership.

Modernizing Federal IT will enhance mission effectiveness and reduce mission risks through a series of complementary initiatives that will drive sustained change in Federal technology, deployment, security, and service delivery.

Enhance Federal IT and Digital Services
Improve the quality and efficiency of critical citizen-facing services by removing the barriers for rapidly adopting the best-in-class commercial solutions to better meet the needs of citizens.

Reduce Cybersecurity Risks to the Federal Mission
Mitigate the impact of risks to Federal agencies' data, systems, and networks by implementing cutting edge cybersecurity capabilities.

Build a Modern IT Workforce
Enable agencies to develop and empower an IT workforce with the skills to achieve modernization goals and support up-to-date technology.

Enhance the effectiveness and efficiency of government services, leveraging data-driven, customer-focused strategies to modernize legacy systems, consolidate common agency services, adopt new shared service models, and embrace commercial cloud solutions.

Strategies

Outcomes

Removing Barriers, Accelerating Adoption
Reduce policy and process burdens to help agencies integrate enhanced technologies to improve the delivery of services to the Government's customers.

- Enable enhanced, secure computing Solutions
- Drive technology modernization Projects
- Streamline system authorization

Modernize Federal IT Delivery
Shift Government to a modern IT service delivery underpinned by user satisfaction and the provision of services by those poised to provide them.

- Modernize the services model
- Focus on the user
- Strengthen identity management
- Prioritize HVA modernization

Embrace Modern Technology Solutions
Adopt new and innovative technologies to deliver services more efficiently, effectively, and readily.

- Adopt cost-effective technology solutions
- Promote access to shared solutions

Federal access to innovative technologies has been hampered by outdated policies and IT acquisition processes. The Removing Barriers, Accelerating Adoption strategy is designed to help agencies adopt advanced technology solutions to better deliver services to the public.

The following milestones will modernize the acquisition of Federal IT services, alleviate policy obstructions, and move away from compliance-based processes:

Strategic Outcome	Key Milestones	Milestone Due Date	Milestone Status	Owner
Enable Enhanced, Secure Computing Solutions: Empower agencies to utilize the full benefits of secure cloud-based computing solutions to strategically drive mission objectives. This includes updating to better enable smart, risk-based decisions before performance measures can be captured.	OMB has issued the Cloud Smart strategy document	Q3FY19	Complete	OMB, DHS, GSA
	OMB has issued an updated DCOI policy memo		Complete	
	OMB has issued a Trusted Internet Connection (TIC) policy update	Q4FY19	Complete	
Drive Technology Modernization Projects: Provide flexible means by which agencies can finance and undertake IT modernization projects through avenues such as the TMF, working capital funds, and regular appropriations.	The Technology Modernization Board has allocated appropriated funds to a broad portfolio of projects of varying risk levels	Q4FY20	On track	Agencies, Board
	100% of TMF project repayment schedules are on time		On track	
	100% of TMF project completion schedules are on time		On track	
Streamline System Authorization: Replace drawn out compliance-based system authorization processes with nimble, risk-based decision making to drive effective and cost-effective utilization of commercial technology.	FedRAMP will issue a feasibility assessment for both the security requirements normalization and the agile authorization pilots.	Q2FY19	Complete	Agencies, OMB, GSA
	Pilots for both of these initiatives will begin with select agencies.	Q4FY19	Complete	
	FedRAMP, with OMB engagement, will conduct a feasibility assessment for the development of the Cyber Cloud Corps.	Q1FY20	Complete	
	Develop a threat-based authorization approach for FedRAMP authorization that maps security requirements to threat	Q1FY21	On track	
	Complete pilot to leverage OSCAL (Open Security Assessment Language) to automate portions of the FedRAMP authorization process	Q2FY22	On track	

Modernizing Federal IT requires a reassessment of the way the Government currently delivers IT services and how it can be improved. The Modernize the Federal IT Delivery Model strategy places a focus on the user experience and promotes the idea that services should be provided by those best suited to achieve the mission.

The following milestones will drive an increased focus on usability of Federal IT and information services and reduce the fragmentation of Federal cybersecurity:

Strategic Outcome	Key Milestones	Milestone Due Date	Milestone Status	Owner
Strengthen Identity Management: Enable agencies to implement modern and privacy-enhancing identity, access, and credentialing technologies that align with industry-leading practices.	OMB has issued a draft identity policy for public comment	Q3FY18	Complete	OMB
	OMB has issued a final identity policy (OMB M-19-17)	Q2FY19	Complete	
	CFO Act Agencies designate an integrated agency-wide ICAM office, team, or other governance structure in support of Enterprise Risk Management capability to effectively govern and enforce ICAM efforts.	Q2FY21	On Track	CFO Act Agencies
	CFO Act Agencies publish a single comprehensive agency-wide ICAM policy, process, and technology solution roadmap, consistent with agency authorities and operational mission needs.	Q2FY21	On Track	CFO Act Agencies
	CFO Act Agencies establish authoritative solutions for ICAM services that can work across the agency.	Q4FY21	On Track	CFO Act Agencies
Prioritize High Value Asset (HVA) Modernization: Promote the modernization and security of the Federal Government's highest value information assets in a prioritized fashion.	DHS has issued updated guidance on HVA classification and protection (BOD 18-02)	Q3FY18	Complete	DHS
	OMB has issued an update to current HVA guidance (OMB M-19-03)	Q4FY18	Complete	OMB
	A Federal strategy is set forth to categorize high value data (see Action 5 of the Federal Data Strategy)	Q4FY20	Complete	OMB

The Government must work to adopt technologies that are not only more efficient, but deliver services to the public in a way that focuses on the user. The Embrace Modern Technology Solutions strategy seeks to promote the adoption of innovative technology solutions to drive efficiency.

The following milestones will drive the development and integration of advanced technology solutions:

Strategic Outcome	Key Milestones	Milestone Due Date	Milestone Status	Owner
Adopt Cost-Effective Technology Solutions: Increase the utilization of technology which drives greater efficiency in the conduct of government business and communication.	75% of civilian CFO Act agencies inboxes utilize cloud-based solutions	Q4FY19	Complete	Agencies
	95%* of civilian CFO Act agencies inboxes utilize cloud-based solutions	Q4FY20	84% At Risk	Agencies
Promote Access to Shared Solutions: Promote the adoption of tools and services that allow the utilization of government economies of scale and service specific expertise. New milestones aligns with DHS' Strengthen Federal Cybersecurity Agency Priority Goal	Aligns together with the Sharing Quality Services CAP Goal			OMB, DHS
	OMB has issued updated Continuous Diagnostic Mitigation (CDM) guidance which enhances the service acquisition model for Phases 2 and 3 (OMB M-19-02, now OMB M-20-04)	Q4FY18	Complete	OMB, DHS
	CDM Phase 3 Event Monitoring tools are made available to 100% of participating agencies	Q4FY19	Completed	OMB, DHS
	100% of CDM agencies have reliable Agency-Wide Adaptive Risk Enumeration (AWARE) scores	Q4FY21	On track	DHS, Agencies
	100% of CDM agencies have established a data connection and begun providing user access data to the Federal CDM Dashboard	Q4FY21	On track	DHS, Agencies

* Based on mission-critical needs, a limited number of agency email inboxes may require on-premise hosting

Mitigate the risk and impact of threats to Federal agencies' data, systems, and networks by implementing cutting-edge cybersecurity capabilities.

STRATEGIES

Manage Asset Security
Implement capabilities that provide observational, analytical, and diagnostic data of an agency's cybersecurity.

Limit Personnel Access
Implement credential and access management capabilities that ensure users only have access to the resources necessary for their job function.

Protect Networks and Data
Implement advanced network and data protection capabilities to protect agency networks and sensitive government and citizen data.

September 2020 Summary of Progress: Reduce Cybersecurity Risks to the Federal Mission
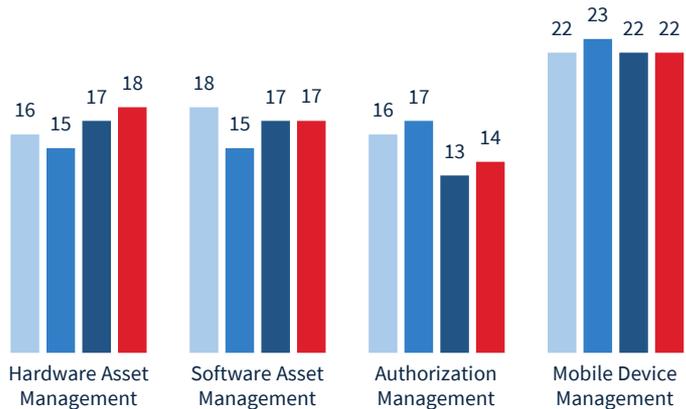
Agencies have made significant progress on implementing key cybersecurity capabilities, addressing the ongoing threats and vulnerabilities to the Federal Mission. For agency level detail, see the [Cybersecurity KPIs]() at performance.gov.
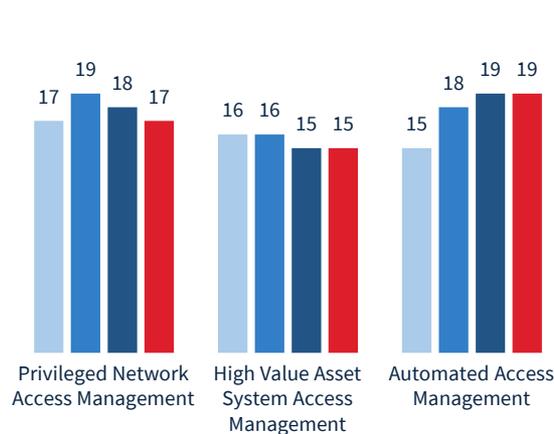
Performance Summary

Number of civilian CFO Act agencies (out of 23) meeting target
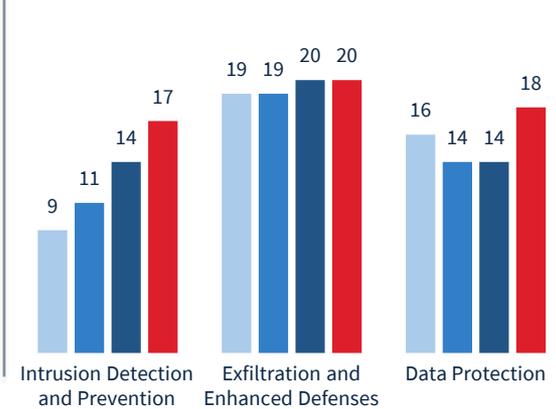
Legend: Q3FY19 | Q4FY19 | Q2FY20 | Q3FY20

Manage Asset Security

Metric	Q3FY19	Q4FY19	Q2FY20	Q3FY20
Hardware Asset Management	16	15	17	18
Software Asset Management	18	15	17	17
Authorization Management	16	17	13	14
Mobile Device Management	22	23	22	22

Limit Personnel Access

Metric	Q3FY19	Q4FY19	Q2FY20	Q3FY20
Privileged Network Access Management	17	19	18	17
High Value Asset System Access Management	16	16	15	15
Automated Access Management	15	18	19	19

Protect Networks and Data

Metric	Q3FY19	Q4FY19	Q2FY20	Q3FY20
Intrusion Detection and Prevention	9	11	14	17
Exfiltration and Enhanced Defenses	19	19	20	20
Data Protection	16	14	14	18

PRESIDENT'S MANAGEMENT AGENDA

Implement capabilities to allow agencies to understand the assets and users operating on their networks.

Delays in implementation of government-wide tools have led to uneven implementation of these capabilities. All agencies will seek to meet the following targets by 2020:

Key Milestones	Milestone Due Date	Milestone Status	Change from last quarter	Owner	Anticipated Barriers or other Issues Related to Milestone Completion
Hardware Asset Management: 95% of the organization's unclassified network has implemented a technology solution to detect and alert upon connection of unauthorized hardware assets.	Q4FY20	At risk	18 agencies met (1 more)	Agencies, OMB	*Delays in implementation of government-wide tools have led to uneven implementation of ISCM capabilities*
Software Asset Management: 95% of the organization's assets are covered by a capability that is able to detect unauthorized software and alert appropriate security personnel.	Q4FY20	At risk	17 agencies met	Agencies, OMB	*Delays in implementation of government-wide tools have led to uneven implementation of ISCM capabilities*
Authorization Management: 100% of High and Moderate Impact Systems are covered by a valid security ATO.	Q4FY20	At risk	14 agencies met (1 more)	Agencies, OMB	*Agencies continue to have a small number of systems which do not have ATO*
Mobile Device Management: 95% of mobile devices are covered by a capability to remotely wipe contents if the device is lost or compromised.	Q4FY20	On track	22 agencies met	Agencies, OMB	

PRESIDENT'S MANAGEMENT AGENDA

Credential and access management capabilities allow agencies to understand who is on their networks and limit users' access to the information necessary to perform their work.

The updated strategy moves from a focus on multifactor authentication (FY 2012 - FY 2017) to the more advanced issue of access management. All agencies will seek to meet the following targets by 2020:

Key Milestones	Milestone Due Date	Milestone Status	Change from last quarter	Owner	Anticipated Barriers or other Issues Related to Milestone Completion
Privileged Network Access Management: 100% of privileged users are required to use a PIV card or AAL3 multifactor authentication method to access the agency's network.	Q4FY18	Missed	17 agencies met (1 fewer)	Agencies, OMB	*Complications related to Covid-19 have required agencies to implement mitigating controls*
High Value Asset System Access Management: 90% of High Value Assets require all users to authenticate using a PIV card or AAL3 multifactor authentication method.	Q4FY20	At risk	15 agencies met	Agencies, OMB	*Some legacy HVA systems remain difficult to implement PIV*
Automated Access Management: 95% of users are covered by an automated, dynamic access management solution that centrally tracks access and privilege levels.	Q4FY20	On track	19 agencies met	Agencies, OMB	*Decentralized identity management at agencies is a significant impediment to improving access management*

Key Milestones:
Protect Networks and Data

Advanced network and data protection capabilities defend agency networks and systems from malicious actors and the potential loss of government information.

The three components of Intrusion Detection and Prevention, Exfiltration and Enhanced Defenses, and Data Protection are new, and agencies will seek to meet the following targets by 2020:

Key Milestones	Milestone Due Date	Milestone Status	Change from last quarter	Owner	Anticipated Barriers or other Issues Related to Milestone Completion
Intrusion Detection and Prevention: At least 4 of 6 Intrusion Prevention metrics have met an implementation target of at least 90% and 100% of email traffic is analyzed using DMARC email authentication protocols.	Q4FY20	At risk	17 agencies met (3 more)	Agencies, OMB	*Agencies are working to complete activities related to BOD 18-01*
Exfiltration and Enhanced Defenses: 90% of outbound communications traffic is checked at the external boundaries to detect potential unauthorized exfiltration of information.	Q4FY20	On track	20 agencies met	Agencies, OMB	
Data Protection: At least 4 of 6 Data Protection metrics have met an implementation target of at least 90%.	Q4FY20	At risk	18 agencies met (2 more)	Agencies, OMB	*Agencies continue to implement key capabilities in HVAs*

Enable Federal agencies to build a workforce with modern technology skills.

STRATEGIES

Assess and Plan
Identify workforce position and skill gaps using better data and develop strategies to address those gaps.

Recruit and Retain Exceptional Talent
Recruit and retain top talent by offering competitive pay and workplace flexibilities.

Reskill the Workforce
Identify existing programs or leverage new programs to offer opportunities for employees to develop new skills to better address future Government and citizen needs.

Invest in recruiting, retaining, and reskilling IT and cybersecurity talent to support mission outcomes and deliver more effective, efficient, and secure Government services.

The following milestones will enhance the Federal IT and Cybersecurity workforce:

Key Milestones	Milestone Due Date	Milestone Status	Owner	Anticipated Barriers or other Issues Related to Milestone Completion
All agencies identify and quantify workforce positions and critical needs using the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework per P.L. 114-113.	Q4FY18	Complete	Agencies, OPM, OMB,	
OPM will provide agencies Federal Employment Viewpoint Survey and other workforce data to aid in workforce planning. OPM, in collaboration with CHCO and CIO councils, will develop a standard dashboard to be used by all agencies to track and analyze workforce data that facilitates agile operations.	Q4FY18	Complete	Agencies, OPM, OMB,	
Each agency finalizes coding cybersecurity positions and declaring cybersecurity work roles of critical need to OPM, in accordance with the Cybersecurity Workforce Assessment Act.	Q4FY19	Complete	Agencies, OPM, OMB	
Establish a reskilling process to train federal employees from diverse backgrounds in IT and cybersecurity skills.	Q1FY21	On track	Agencies, OPM, OMB	
Develop a market-informed pay and compensation strategy for cybersecurity and other mission critical IT positions to improve recruitment and retention.	Q4FY21	On track	Agencies, DHS, OMB	
Develop a centralized training capability for all cybersecurity personnel across the Federal workforce.	Q4FY21	On track	Agencies, OPM, OMB	

Lead - Executive Office of the President

Office of Management and Budget (OMB)

LEAD:

Maria Roat, Deputy Federal Chief Information Officer

KEY PERSONNEL:

Peter Warren, Associate Director for Personnel and Performance Management

Matt Cutts, Administrator, US Digital Services

Paul Ray, Administrator, Office of Information and Regulatory Affairs

---

Supporting Agencies

General Services Administration (GSA)

LEAD:

Emily Murphy, Administrator of General Services Administration

KEY PERSONNEL:

Allison Brigati, Deputy Administrator of General Services Administration

Julie Dunne, Acting Commissioner, Federal Acquisition Service

Anil Cheriyan, Deputy Commissioner, Technology Transformation

Department of Homeland Security (DHS)

LEAD:

Christopher Krebs, Director, Cybersecurity and Infrastructure Security Agency

KEY PERSONNEL:

Bryan Ware, Deputy Director, Cybersecurity and Infrastructure Security Agency

CAP Partner Agency

Department of Agriculture (USDA)

LEAD:

Steve Censky, Deputy Secretary

KEY PERSONNEL:

Gary Washington, Chief Information Officer

Department of Homeland Security

Numerous DHS programs support the reduction of cybersecurity risk. DHS has established an FY 2020-2021 Agency Priority goal (APG) to Strengthen Federal Cybersecurity.

- The APG measures the effectiveness of several DHS cybersecurity programs, including: Continuous Diagnostics and Mitigation (CDM), National Cybersecurity Protection System (NCPS), the High Value Asset Program, Cyber Hygiene Scanning, and Hunt and Incident Response Teams (HIRT).
- DHS provides tools and services that supports this CAP Goal that help agencies achieve the cybersecurity targets set forth in this CAP goal.

General Services Administration

The digitization of websites and services relies on GSA as a close partner to help Federal agencies acquire and adopt modern IT products and services.

- Federal Acquisition Service (FAS)
  - Technology Transformation Service (TTS)
- Office of Government-wide Policy (OGP)

Interagency Councils

- CIO Council
- CHCO Council
- CISO Council
- Small and Micro Agency Council

Department of Commerce

- National Institute of Standards and Technology (NIST)

Office of Personnel Management

- Employee Services (ES)

ATO - Authority to Operate

BOD - Binding Operational Directive

CDM - Continuous Diagnostics and Mitigation

CFO - Chief Financial Officer

CHCO - Chief Human Capital Officer

CIO - Chief Information Officer

DCOI - Data Center Optimization Initiative

DHS - Department of Homeland Security

DMARC - Domain Message Authentication Reporting & Conformance

FedRAMP - Federal Risk and Authorization Management Program

GSA - General Services Administration

HVA - High Value Asset

ICAM - Identity, Credential, and Access Management

ISCM - Information Security Continuous Monitoring

KPI - Key Performance Indicators

NICE Framework - National Initiative for Cybersecurity Education Framework

NIST - National Institute of Standards and Technology

OMB - Office of Management and Budget

OPM - Office of Personnel Management

TIC - Trusted Internet Connection

TMF - Technology Modernization Fund