PRESIDENT'S MANAGEMENT AGENDA

CAP Goal Action Plan

Modernize IT to Increase Productivity and Security

Goal Leaders

Steve Censky, Deputy Secretary, United States Department of Agriculture

Suzette Kent, Federal Chief Information Officer, Office of Management and Budget

September 2018

Overview

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.

Goal Pillars

A multi-pronged IT modernization strategy between OMB and Agency Partners to achieve the desired results this Administration expects and our citizens deserve.

Realize the recommendations made in the **Report to the President on Federal IT Modernization** in order to enhance the functionality of citizen services and drive cost efficiencies of Government operations.

Implement the **Modernizing Government Technology Act** to enable agencies to establish IT working capital funds that can direct cross-agency dollars to IT modernization projects, and establishing a centralized fund that will invest in modernization.

Develop a new **Federal cloud adoption strategy** to provide agencies the guidance and flexibilities needed to move safely, securely and rapidly to the cloud and decommission antiquated internal agency systems.

Strengthen the Federal cybersecurity posture in order to **protect valuable information systems**, aligning agency security outcomes with Federal cybersecurity strategies.

Collaborate with the Office of American Innovation and the General Services Administration to establish **Centers of Excellence** to provide technical expertise and strategic acquisition support to help agencies perform top to bottom modernization activities.

Work with the Office of Personnel Management to fundamentally overhaul our recruitment, retention, and reskilling strategies to bring **more top technical talent** into the Government, improve the technology and cybersecurity capabilities of our current workforce.

Goal Structure

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.

FY18Q3 Summary of Progress: Enhance Federal IT and Digital Services

Many of these activities are still in the early phases of development, requiring updated guidance to be issued to set expectations and requirements for agency implementation. The following progress has been made thus far:

- Approximately 61% of civilian CFO Act agency email inboxes are now serviced by cloud-based solutions (August 2018)
- DHS issued a Binding Operational Directive providing Federal agencies with updated guidance on the identification of high value assets (HVAs).
- Two full-scale Trusted Internet Connection (TIC) pilots have completed activities, with several smaller scale pilots still underway; DHS has also drafted an update to the TIC Strategy.
- The Technology Modernization Fund (TMF) awarded funding for three projects totaling $45 million.
- OMB collected input from the public on its draft Federal identity policy, receiving feedback from over 500 individuals and organizations. OMB is currently incorporating the public's feedback.
- Twenty of 23 Federal civilian CFO Act agencies are now sharing cybersecurity information between their agency-level dashboards and the DHS CDM Federal Dashboard

FY18Q3 Summary of Progress: Reduce Cybersecurity Risks to the Federal Mission

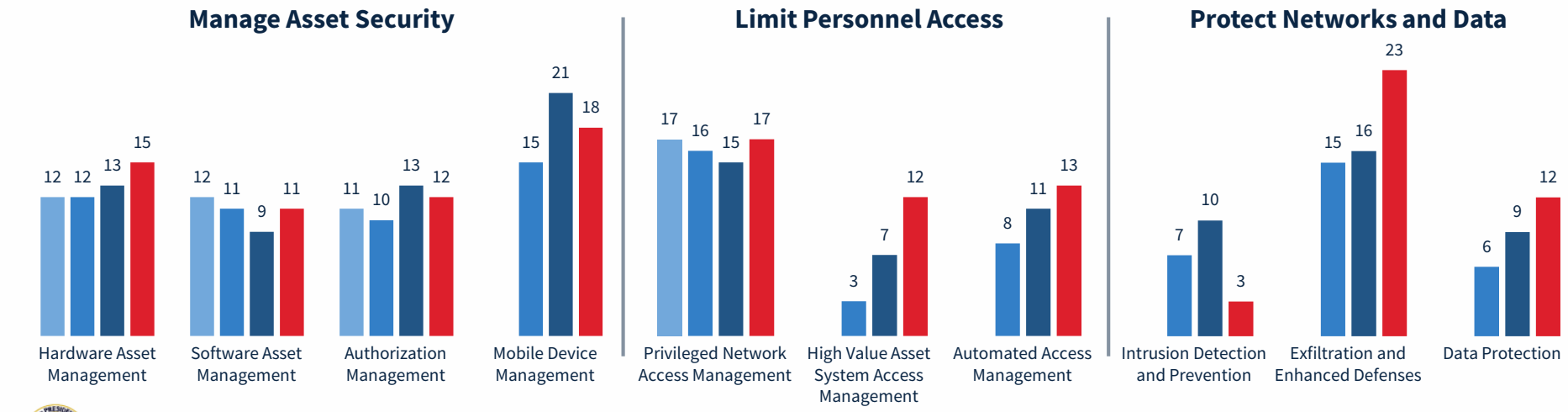
Agencies continue to make progress in implementing key cybersecurity capabilities, addressing the ongoing threats and vulnerabilities to the Federal Mission. For agency level detail, see the Cybersecurity KPIs at performance.gov

OMB and DHS, in collaboration with agency partners, reviewed and updated the FISMA CIO metrics to ensure alignment with the priorities outlined in the *Report to the President on Federal IT Modernization,* other sections of the President's Management Agenda.

These changes (effective July 2018) included a greater focus on HVAs and enterprise-level visibility of information, but also removed duplicative or unassessed metrics in order to reduce burden. As a result of these changes, the number of agencies meeting particular metrics may have shifted.

Performance Summary

Number of civilian CFO Act agencies (out of 23) meeting target



FY18Q3 Summary of Progress: Build a Modern IT Workforce

Many workforce activities are still in the early phases of development, requiring updated guidance to be issued to set expectations and requirements for agency implementation. The following progress has been made thus far:

Implementation of the Federal Cybersecurity Workforce Assessment Act

- Agencies completed initial identification and coding of federal civilian positions performing information technology, cybersecurity, or other cyber-related functions. OPM has requested additional, more detailed data from agencies beyond the original request and has extended the deadline.
- OPM has issued guidance for identifying, addressing, and reporting critically needed cybersecurity work roles

Human Capital Strategic Planning

- Agencies are currently completing updates to their Human Capital Strategic Plans to align with the President's Management Agenda and Agency Priority Goals
- OMB and OPM continue to work collaboratively with federal agencies to identify successful recruitment, retention, and reskilling initiatives that may be piloted government-wide.

Chief Information Officer (CIO) and Chief Human Capital Officer (CHCO) Councils

- The CIO and CHCO councils are working jointly to develop and execute on federal workforce initiatives for FY18 and FY19. Additional updates may be found at CIO.gov and/or CHCO.gov.
- The CIO Council has engaged multiple academic institutions to explore existing IT and cybersecurity curriculums available to federal employees.
- Private sector engagement options are being explored to evaluate other federal education and training opportunities.

Market-Informed Pay

- DHS and OPM working toward a market-informed pay and compensation system for DHS cybersecurity personnel

Goal Structure: Enhance Federal IT and Digital Services

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 more readily.	• Adopt Cost-Effective Technology Solutions • Promote Access to Shared Solutions

Key Milestones: Removing Barriers, Accelerating Adoption

Many of these activities are still in the early phases of development, requiring updated guidance to be issued to set expectations and requirements for agency implementation. The following progress has been made thus far:

Enable Modern, Secure Computing Solutions

- Two full-scale Trusted Internet Connection (TIC) pilots have completed activities, with several smaller scale pilots still underway
- DHS presented a draft updated TIC Strategy to the interagency TIC Modernization Working Group and is collecting feedback from agencies on revisions to the TIC Reference Architecture and Use Cases

Drive Adoption of Technology Modernization Projects

- The Technology Modernization Fund (TMF) awarded funding for three projects totaling $45 million (for more information see https://tmf.cio.gov/projects/)
- The Technology Modernization Board continues to review applications for high priority projects

Streamline System Authorization

- OMB and GSA are evaluating the feasibility of common government-wide security requirements above the current FedRAMP baseline that incorporates agency-specific requirements
- OMB and GSA are also developing a process to better incorporate agile methodologies into the ATO process, providing a more flexible approach for Federal agencies and cloud service providers

Key Milestones: Removing Barriers, Accelerating Adoption

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 telecom services, alleviate policy obstructions, and move away from compliance-based processes:

Strategic Outcome	Near Term 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 an update to current Cloud Strategy document	Q4FY18	On track	OMB, DHS, GSA
	OMB has instituted standard cloud contracting guidance		On track	
	OMB has rationalized the Data Center Optimization Initiative (DCOI) with the Cloud Strategy		On track	
	Update TIC/EINSTEIN structure to accommodate new cloud access options		On track	
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	
	Through increased engagement with agency CIOs, fully rationalize modernization to the application level	Q4FY20	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***.	OMB, DHS, and GSA have issued a strategic plan for streamlining ATO processes, including FedRAMP, based on common needs	Q4FY18	On track	Agencies, OMB, GSA

Key Milestones: Modernize the Federal IT Delivery Model

Many of these activities are still in the early phases of development, requiring updated guidance to be issued to set expectations and requirements for agency implementation. The following progress has been made thus far:

Modernize the Services Model

- GSA, OMB, and DHS developed an initial acquisition strategy and began work on a public solicitation for feedback on the potential SOC as a Service capability requirements.
- OMB and DHS began outreach to Federal agencies to identify potential SOC as a Service customers as well as potential Centers of Excellence.

Focus on the User

- OMB is working with agency partners to determine the best way to utilize digital analytics to drive improved customer experience

Strengthen Identity Management

- OMB collected input from the public on its draft Federal identity policy, receiving feedback from over 500 individuals and organizations. OMB is currently incorporating the public's feedback.

Prioritize High Value Asset (HVA) Modernization

- DHS issued a Binding Operational Directive providing Federal agencies with updated guidance on the identification of HVAs.
- Agencies submitted updated lists of their HVAs to DHS and OMB for analysis and prioritization.

Key Milestones: Modernize the Federal IT Delivery Model

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	Near Term Key Milestones	Milestone Due Date	Milestone Status	Owner
Modernize the Services Model: Improve the way services are provisioned within the government, ***promoting models in which under performing or under resourced agencies can purchase services elsewhere***. SOC as a Service will be used as a test case.	OMB has issued updated CPIC guidance which includes staffing and resourcing of agency Security Operation Centers (SOCs)	Q3FY18	Complete	OMB, GSA
	OMB has issued a questionnaire to gauge the effectiveness of select agency SOCs	Q3FY18	Complete	
	GSA has issued an RFI regarding provision of SOC services from private sector entities	Q4FY18	On track	
	OMB has named a Federal SOC Center of Excellence	Q4FY18	On track	
Focus on the User: Encourage the ***use of user centered design in the development of Federal IT products and digital services***, including capturing reliable and actionable information to improve overall user experience.	Metrics and assessment criteria to determine the extent to which agencies are utilizing customer feedback to improve the delivery of digital services have been established	Q4FY18	On track	OMB, GSA
	Federal design standards and best practices for user centered design for Federal websites and digital service have been issued	Q4FY19	On track	OMB, GSA
	Aligns with the Improving Customer Experience CAP Goal			OMB
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	Q4FY18	On track	
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	Q3FY18	Complete	DHS
	OMB has issued an update to current HVA guidance	Q4FY18	On track	OMB
	A Federal strategy is set forth to categorize high value data	Q4FY19	On track	OMB

Key Milestones: Embracing Modern Technology Solutions

Many of these activities are still in the early phases of development, requiring updated guidance to be issued to set expectations and requirements for agency implementation. The following progress has been made thus far:

Adopt Cost-Effective Technology Solutions

- Approximately 61% of civilian CFO Act agency email inboxes are now serviced by cloud-based solutions (August 2018). For a complete readout by agency, see IT Modernization KPIs at performance.gov

Promote Access to Shared Security Solutions

- Twenty of 23 Federal civilian CFO Act agencies are now sharing cybersecurity information between their agency-level dashboards and the DHS CDM Federal Dashboard, which provides government-wide situational awareness
- A total of 12 agencies are now covered by task orders for CDM DEFEND, the new generation of cybersecurity capability acquisition designed to provide agencies with more flexibility in selecting the tools they use to protect their networks and information

Key Milestones: Embrace Modern Technology Solutions

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 improved outcomes for the customer.

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

Strategic Outcome	Near Term 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	On track	Agencies
	95%* of civilian CFO Act agencies inboxes utilize cloud-based solutions	Q4FY20	On track	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.	Aligns together with the Sharing Quality Services CAP Goal			OMB
	OMB has issued updated Continuous Diagnostic Mitigation (CDM) guidance which enhances the service acquisition model for Phases 2 and 3	Q4FY18	On track	
	OMB, GSA, and their Federal partners have established guidance for the rationalization of shared IT services as more become available	Q4FY19	On track	OMB, GSA, Others

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

Goal Structure: Reduce Cybersecurity Risks to the Federal Mission

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.

Key Milestones: Manage Asset Security

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

Changes in metrics (effective July 2018) included a greater focus on HVAs. As a result of this change, the number of agencies meeting particular metrics may have shifted.

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 hardware assets are covered by a capability to detect and alert upon the connection of an unauthorized hardware asset	Q4FY20	On track	Better, 15 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 software assets are covered by a whitelisting capability	Q4FY20	On track	Better, 11 agencies met (2 more)	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	On track	Worse, 12 agencies met (1 fewer)	Agencies, OMB	
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	Worse, 18 agencies met (3 fewer)	Agencies, OMB	*Agencies have re-evaluated implementation of this metric based on OMB clarification in recent metrics update*

*These milestones represent key areas within the Federal Information Security Modernization Act of 2014 (FISMA) Chief Information Officer metrics. DHS programs, including Continuous Diagnostics and Mitigation (CDM) and EINSTEIN, may provide some of these capabilities to agencies.

Key Milestones: Limit Personnel Access

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.

Changes in metrics (effective July 2018) included a greater focus on HVAs. As a result of this change, the number of agencies meeting particular metrics may have shifted.

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	On track	Better, 17 agencies met (2 more)	Agencies, OMB	*Overall Federal implementation is currently approximately 99%, with small numbers of privileged users still awaiting appropriate credentials*
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	On track	Better, 12 agencies met (5 more)	Agencies, OMB	*Updates to metrics guidance have shifted this metric from high impact systems to HVAs; OMB is in the process of updating guidance regarding the protection of HVAs*
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	Better, 13 agencies met (2 more)	Agencies, OMB	*Decentralized identity management at agencies is a significant impediment to improving access management*

* These milestones represent key areas within the Federal Information Security Modernization Act of 2014 (FISMA) Chief Information Officer metrics. DHS programs, including Continuous Diagnostics and Mitigation (CDM) and EINSTEIN, may provide some of these capabilities to agencies.

** This is a continuation of the FY 2015-2017 Cybersecurity CAP Goal; as such, agencies are expected to complete this metric by Q4FY18

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.

Changes in metrics (effective July 2018) included a greater focus on HVAs and enterprise-level visibility of information. As a result of these changes, the number of agencies meeting particular metrics may have shifted.

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	On track	Worse, 3 agencies met (7 fewer)	Agencies, OMB	*Updated metrics required many controls to be 'centrally visible at the enterprise level'; agencies are in the process of implementing BOD 18-01*
Exfiltration and Enhanced Defenses: At least 3 of 4 Exfiltration and Enhanced Defenses metrics have met an implementation target of at least 90%	Q4FY20	On track	Better, 23 agencies met (7 more)	Agencies, OMB	*Shift in focus from high and moderate impact systems to HVAs required the removal of one metric. With high agency implementation in this area, OMB intends to improve this target to 4 of 4 metrics in the future.*
Data Protection: At least 4 of 6 Data Protection metrics have met an implementation target of at least 90%	Q4FY20	On track	Better, 12 agencies met (3 more)	Agencies, OMB	*Shift in focus from high and moderate impact systems to HVAs required the removal of one metric.*

*These milestones represent key areas within the Federal Information Security Modernization Act of 2014 (FISMA) Chief Information Officer metrics. DHS programs, including Continuous Diagnostics and Mitigation (CDM) and EINSTEIN, may provide some of these capabilities to agencies.

Goal Structure: Build a Modern IT Workforce

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

STRATEGIES

Assessment and Planning
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.

Key Milestones: Build a Modern IT Workforce

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	Change from last quarter	Owner	Anticipated Barriers or other Issues Related to Milestone Completion
All agencies identify and quantify workforce positions and skill gaps using the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework per P.L. 114-113	Q4FY18	On track	Better	Agencies, OPM, OMB,	*OPM has requested additional, more detailed data from agencies beyond the original request and has extended the deadline*
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	On track	Better	Agencies, OPM, OMB,	
Each agency CIO and CHCO must jointly identify two position or skills gap priorities and incorporate them into to the agency's Human Capital Operating Plan, which will be shared with OMB. Actions to address these two gaps must be executed no later than FY19	Q1FY19	On track	Better	Agencies, OPM, OMB	
Engage industry and academia to develop Federal workforce planning strategies that include initiatives to reskill and redeploy the existing workforce to achieve mission results. The CHCO and CIO councils shall jointly present recommendations to OMB no later than FY19	Q2FY19	On track	Better	Agencies, OPM, OMB, CIO Council, CHCO Council	
Develop a market-informed pay and compensation strategy for cybersecurity and other mission critical IT positions to improve recruitment and retention	Q2FY19	On track	Better	Agencies, OPM, OMB	

Lead - Executive Office of the President

Office of Management and Budget (OMB)

LEAD:

Suzette Kent, Federal Chief Information Officer

KEY PERSONNEL:

Margie Graves, Deputy Federal Chief Information Officer

Grant Schneider, Acting Federal Chief Information Security Officer; Senior Director - Homeland, NSC Cybersecurity Directorate

Peter Warren, Associate Director for Personnel and Performance Management

U.S. Digital Service (USDS)

LEAD:

Matt Cutts, Acting Administrator

KEY PERSONNEL:

Eddie Hartwig, Deputy Administrator

Supporting Agencies

General Services Administration (GSA)

LEAD:

Emily Murphy, Administrator of General Services

KEY PERSONNEL:

Allison Brigati, Deputy Administrator

Alan Thomas, Commissioner, Federal Acquisition Service

Joanne Collins-Smee, Deputy Commissioner, Technology Transformation Service

Department of Homeland Security (DHS)

LEAD:

Christopher Krebs, Undersecretary Nominee, National Programs and Protection Directorate

KEY PERSONNEL:

Jeanette Manfra, Assistant Secretary, Cybersecurity and Communications (CS&C)

Richard Driggers, Deputy Assistant Secretary, CS&C

Mark Kneidinger, Director, Federal Network Resilience

CAP Partner Agency

Department of Agriculture (USDA)

LEAD:

Steve Censky, Deputy Secretary

KEY PERSONNEL:

Gary Washington, Chief Information Officer

Contributing Programs

Department of Homeland Security

Numerous DHS programs support the Reduce Cybersecurity Risks to the Federal Mission strategy. DHS has established an Agency Priority goal (APG) to Strengthen Federal Cybersecurity with the FY 2019 President's Budget.

- 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' APG supports this CAP Goal by providing tools and services that help agencies achieve the targets set forth in all three components of the Reduce Cybersecurity Risks strategy.

General Services Administration

The Modernize the Stack and Embrace Cloud Solutions portion of the CAP Goal rely 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)

U.S. Department of Agriculture

- IT Modernization Partner