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

June 2019

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.

June 2019 Summary of Progress: Enhance Federal IT and Digital Services

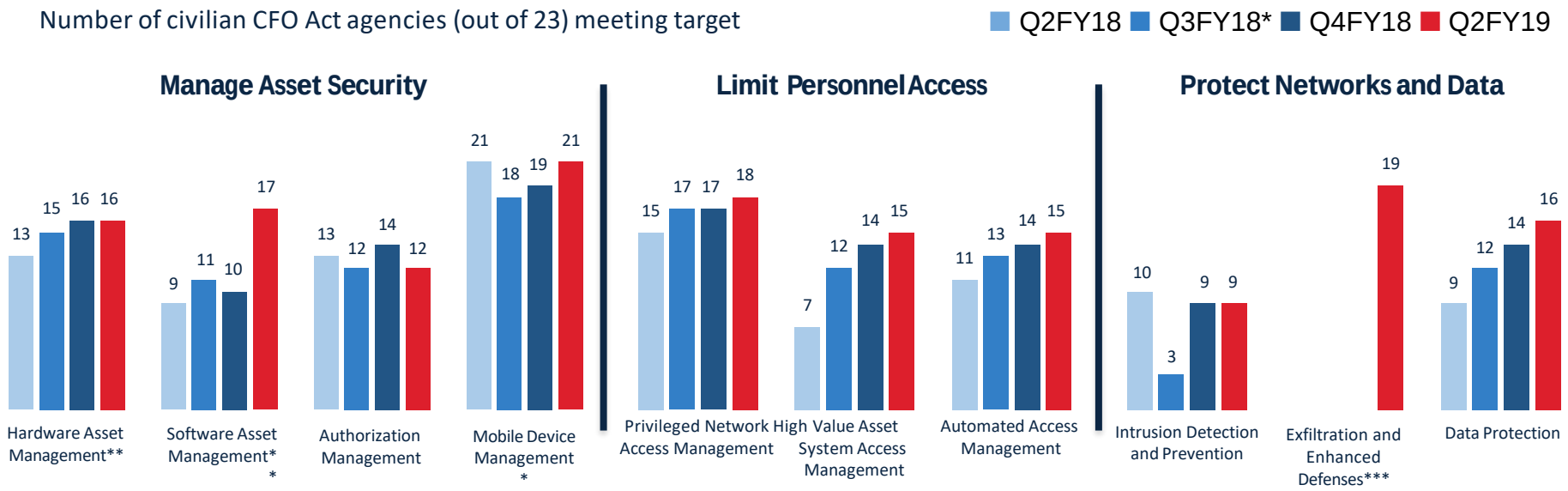
- Approximately 75% of civilian CFO Act agency email inboxes are now serviced by cloud-based solutions (May 2019).
- The Technology Modernization Fund (TMF) awarded funding for seven projects totaling almost $90 million (for more information see https://tmf.cio.gov/projects/) The TMF Board continues to review applications for high priority projects.
- OMB issued M-19-17, which enacts a common vision for Identity, Credential and Access Management (ICAM) as an enabler of mission delivery, trust, and safety of the Nation.
- OMB and GSA are evaluating the best mechanisms for normalizing Federal security requirements and prioritizing control deployment for FedRAMP ATO's.

June 2019 Summary of Progress: Reduce Cybersecurity Risks to the Federal Mission

Agencies continue to make 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



* In July of 2018, OMB and DHS reviewed and updated the FISMA CIO metrics to include a greater focus on HVAs and enterprise-visibility of information. As a result of these changes, the number of agencies meeting particular metrics may have shifted.

** Due to changes to FY 2019 FISMA CIO metrics the Hardware and Software Asset Management capabilities track the ability to detect and alert upon their respective events. See slide 13 for details.

*** Due to changes to FY 2019 FISMA CIO metrics the Exfiltration and Enhanced Defenses capability cannot be trended and this data now reflects a more ambitious target. See slide 13 for details.

June 2019 Summary of Progress: Build a Modern IT Workforce

Recruiting

- Agencies submitted workforce roles of critical need and action plans in April 2019. OPM is analyzing agencies' submissions and will produce a report on government-wide cybersecurity hiring needs during Summer 2019.
- DHS and OMB will build on OPM's analysis to prioritize areas of government-wide critical need.

Reskilling

- The CIO Council launched the first cohort of the Federal Cybersecurity Reskilling Academy, and closed applications for the second cohort. In total, the CIO Council will reskill 50 people in FY19, and develop a playbook of best practices for agencies to replicate in the future.
- The Council is evaluating opportunities to offer additional reskilling programs in the future.

Cybersecurity Talent Management System

- DHS and OMB are designing a new personnel system that will use innovative techniques to attract, hire, and retain federal cybersecurity personnel.
- DHS is exploring ways to increase the mobility of the cybersecurity workforce.

Workforce Mobility

- OMB is exploring ways to make cybersecurity positions more mobile, including flexibilities that allow workers to easily move from one position to another, or from one agency to another.
- OMB will work with agencies to evaluate the need for additional surge capacity to respond to major cybersecurity incidents, which may include temporary flexibilities for agencies to deploy their cybersecurity personnel as part of an incident response team.

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

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

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 the Cloud Smart strategy document	Q2FY19	On track	OMB, DHS, GSA
	OMB has issued an updated DCOI policy memo		On track	
	OMB has instituted standard cloud contracting guidance	Q4FY19	On track	
	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	
	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***.	FedRAMP will issue a feasibility assessment for both the security requirements normalization and the agile authorization pilots.	Q2FY19	On track	Agencies, OMB, GSA
	Pilots for both of these initiatives will begin with select agencies.	Q3FY19	On track	
	FedRAMP, with OMB engagement, will draft both content and structure of the Cyber Cloud Corps.	Q4FY19	On track	

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 TermKey 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	Q2FY19	Complete	
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	Q4FY19	On track	OMB

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	Complete	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, 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)	Q4FY18	Complete	OMB, DHS
	CDM Phase 3 Event Monitoring tools are made available to 100% of participating agencies	Q4FY19	On track	OMB, DHS

* 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.

Reduce Cybersecurity Risks to the Federal Mission

Changes in FY 2019 FISMA CIO Metrics have resulted in changes to cybersecurity CAP Goal targets. These changes impact two areas:

- **Hardware and Software Asset Management:** In order to provide better clarity into agency cybersecurity posture, FY 2019 FISMA CIO Metrics distinguished between the ability to detect and alert upon an event and the ability to block upon an event. Performance in these metrics will continue to track the ability to detect and alert, as this was the intent of the original CAP Goal target. OMB will evaluate updating these targets to include the ability to block in FY 2020.

- **Exfiltration and Enhanced Defenses:** As of FY 2018Q4, all 23 civilian CFO Act Agencies had met targets for 3 of the 4 metrics in this area. Following the example set forth by the *Shifting From Low-Value to High-Value Work* CAP Goal, collection of these metrics was eliminated to reduce agency reporting burden. The remaining metric (measuring the ability to check network traffic for data exfiltration attempts) will be tracked publicly. As this new target is more ambitious, **OMB considers all agencies to have met the original CAP Goal target.**

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 the organization's unclassified network has implemented a technology solution to detect and alert upon connection of unauthorized hardware assets.	Q4FY20	On track	No change, 16 agencies met	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	On track	Better, 17 agencies met (7 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 (2 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	Better, 21 agencies met (2 more)	Agencies, OMB	

* See slide 13 for details on changes to CAP Goal targets

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, 18 agencies met (1 more)	Agencies, OMB	*Small populations 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, 15 agencies met (1 more)	Agencies, OMB	*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, 15 agencies met (1 more)	Agencies, OMB	*Decentralized identity management at agencies is a significant impediment to improving access management*

* 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	No change, 9 agencies met	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	19 agencies met	Agencies, OMB	
Data Protection: At least 4 of 6 Data Protection metrics have met an implementation target of at least 90%.	Q4FY20	On track	Better, 16 agencies met (2 more)	Agencies, OMB	

* See slide 13 for details on changes to CAP Goal targets

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 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,	
Establish a reskilling process to train federal employees from diverse backgrounds in IT and cybersecurity skills.	Q4FY19	On track	Better	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. OPM produces a report to Congress on the government-wide cybersecurity workforce needs.	Q4FY19	On track	Better	Agencies, OPM, OMB	
Develop a market-informed pay and compensation strategy for cybersecurity and other mission critical IT positions to improve recruitment and retention	Q4FY19	On track	Better	Agencies, OPM, OMB	
Develop a centralized training capability for all cybersecurity personnel acrossthe Federal workforce.	Q4FY21	On track	Better	Agencies, OPM, OMB	

Goal Leadership

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)

S. Department of Agriculture

- IT Modernization Partner

Acronyms

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