Agency Priority Goal Action Plan

Strengthen Federal Cybersecurity

Goal Leader: Jeanette Manfra, Assistant Secretary for Cybersecurity and Communications

Theme: National Defense

Overview

Goal Statement

- Strengthen the defense of the federal network through the increased dissemination of cyber threat and vulnerability information in near real time to federal agencies. By September 30, 2019, federal agencies will mitigate 90% of significant (critical and high) vulnerabilities identified through DHS scanning of their networks within a designated timeline.

Challenge

- Cybersecurity threats to federal networks continue to grow and evolve at an alarming rate.
- Adversaries in cyberspace conduct attacks against federal networks in real time, collecting sensitive data and information in a matter of minutes.
- Securing computer networks of federal agencies is a collaborative effort. Federal agencies must work in close collaboration with DHS to ensure that DHS cybersecurity programs and tools are meeting their needs and evolving alongside the threat.
- Enabling agency use of DHS provided tools and information to take action with the same speed and agility as adversaries is critical.

Opportunity

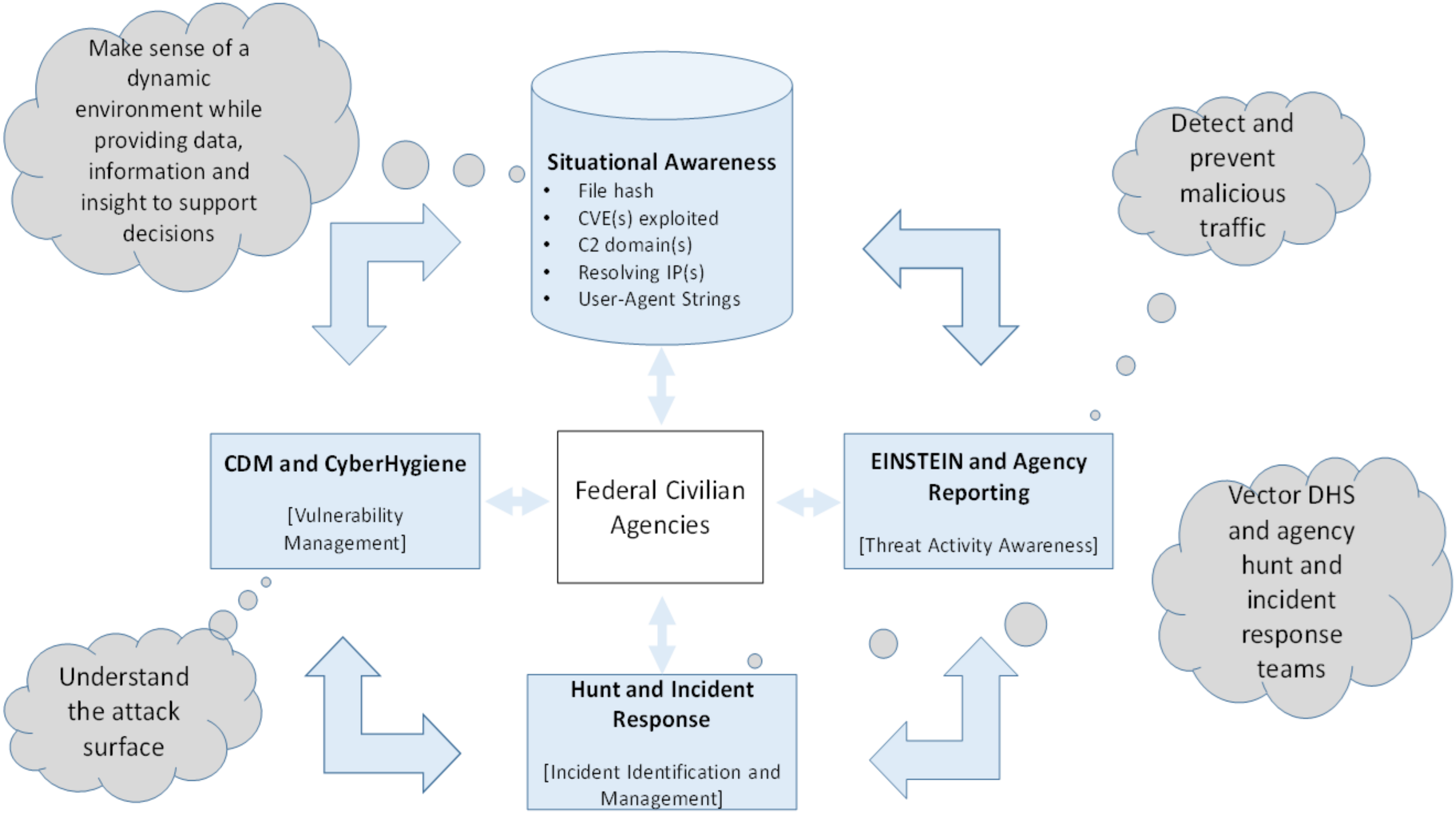
- Continuous scanning, intrusion prevention, and vulnerability assessments allow DHS to provide agencies with the necessary tools and information to take timely and appropriate risk based actions to defend their networks.
- DHS will continue to engage with senior agency leadership and appropriate information technology and security experts to apply cybersecurity programs and agency cybersecurity practices and ensure the successful implementation and use of their capabilities.

Goal Structure & Strategies

Strategies: To effectively strengthen federal network cybersecurity, DHS will coordinate with senior agency leadership to advance agency-level processes and apply the following strategies:

Cyber Hygiene Scanning	Continuous Diagnostics and Mitigation (CDM)	EINSTEIN	High Value Asset (HVA) Assessments	Hunt & Incident Response Team (HIRT)
For a specified time period, DHS will scan an agency's network for vulnerabilities on its external public facing assets and connections and will work with that agency to effectively mitigate them.	CDM will provide agencies with increased awareness of assets, users, and events on their networks by: • Providing an inventory of the hardware and software that is on agency networks. • Providing increased awareness of users on networks to allow agencies to restrict network privileges and access to only those individuals who have a need • Providing insight into what is happening on an agency network.	DHS provides boundary protection to deny entry of malicious activity and actors onto federal networks through EINSTEIN.	In order to focus leadership attention and resources on the security and protection of the most sensitive federal IT systems and data, DHS will provide assessments of identified HVAs on agency networks.	DHS provides a response and detection capability through the HIRT team to assist federal agencies in the event of an actual or suspected cyber incident by utilizing cross-cutting information available from CDM, EINSTEIN, cyber hygiene scanning, and other internal/external sources to perform analysis.

Goal Structure & Strategies



Make sense of a dynamic environment while providing data, information and insight to support decisions

Situational Awareness

- File hash
- CVE(s) exploited
- C2 domain(s)
- Resolving IP(s)
- User-Agent Strings

Detect and prevent malicious traffic

CDM and CyberHygiene

[Vulnerability Management]

Federal Civilian Agencies

EINSTEIN and Agency Reporting

[Threat Activity Awareness]

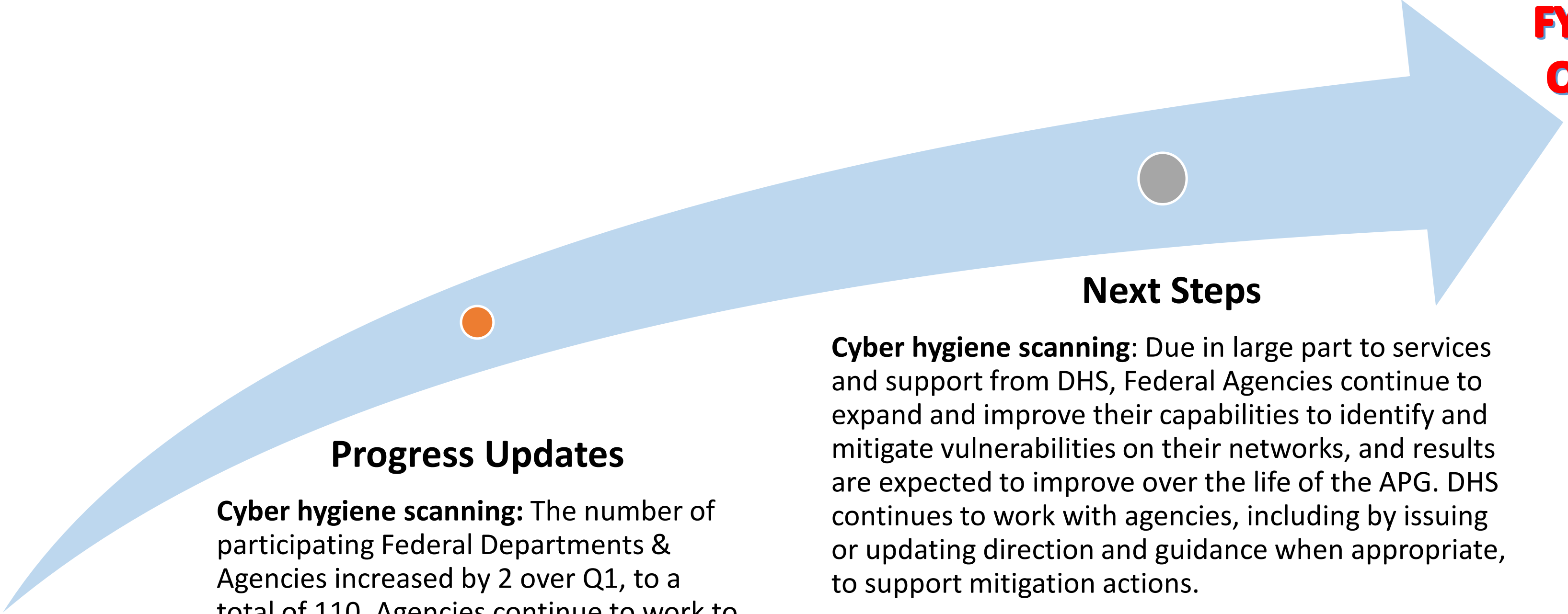
Vector DHS and agency hunt and incident response teams

Understand the attack surface

Hunt and Incident Response

[Incident Identification and Management]

Summary of Progress – FY18 Q2



Progress Updates

Cyber hygiene scanning: The number of participating Federal Departments & Agencies increased by 2 over Q1, to a total of 110. Agencies continue to work to increase their capacity to address the most serious vulnerabilities identified by the enhanced visibility from Cyber Hygiene Scanning.

CDM Deployment: Nine agencies established a connection with the DHS managed Federal Dashboard in Q2.

High Value Assets: Binding Operational Directive (BOD 18-02), Securing High Value Assets (HVAs), was issued on May 7, 2018 to ensure timely remediation of vulnerabilities identified by DHS-led assessments.

Next Steps

Cyber hygiene scanning: Due in large part to services and support from DHS, Federal Agencies continue to expand and improve their capabilities to identify and mitigate vulnerabilities on their networks, and results are expected to improve over the life of the APG. DHS continues to work with agencies, including by issuing or updating direction and guidance when appropriate, to support mitigation actions.

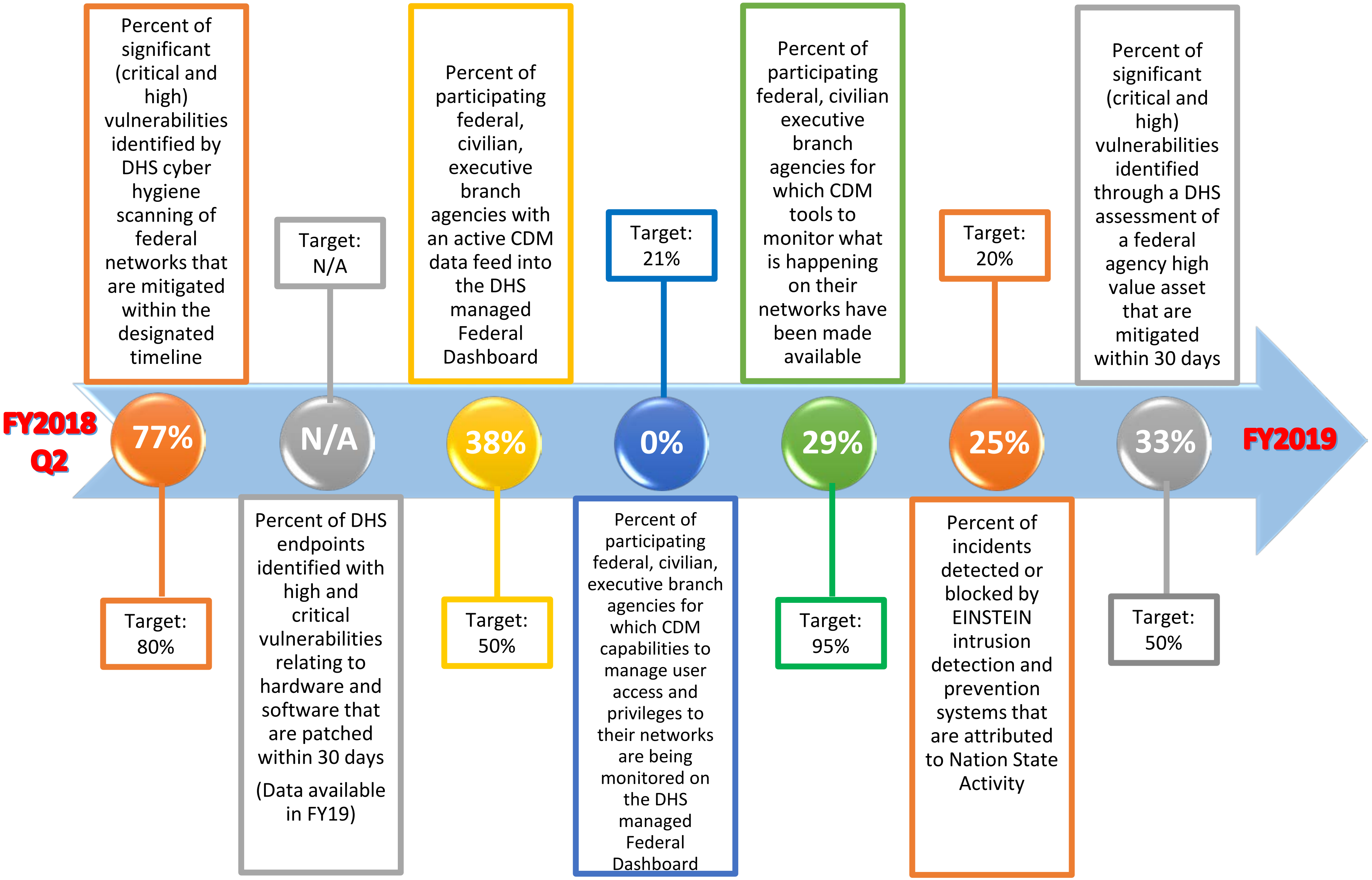
CDM Deployment: The CDM program office anticipates at least five more agencies will establish information exchange connections between the federal and agency dashboards by the end of Q3 FY 2018.

Capabilities to manage user access and privileges to their network will begin to be connected to the dashboard in Q3, with full information exchange with agencies to meet the target expected in Q4.

Key Milestones

Key Milestone	Milestone Due Date	Milestone Status	Comments
First information exchange from an Agency Dashboard to Federal Dashboard	Q1, FY18	Complete	Continuous Diagnostics and Mitigation (CDM) achieved the successful completion of an Information Exchange with the Environmental Protection Agency (EPA) during Q1.
Eight additional information exchanges between Agency Dashboards and the Federal Dashboard	Q2, FY18	Complete	As of Q2 FY 2018, CDM has established information exchange connections with a total of nine Chief Financial Officer Act agencies.
First exchanges of CDM Phase 2 information (user access and privileges) from Agency Dashboards to the Federal Dashboard	Q3, FY18	On Track	
Delivery of Phase 3 capabilities (events on Federal networks) completed for participating agencies	Q4, FY18	On Track	

Key Indicators



FY2018 Q2

77%

Percent of significant (critical and high) vulnerabilities identified by DHS cyber hygiene scanning of federal networks that are mitigated within the designated timeline

Target: 80%

N/A

Target: N/A

Percent of DHS endpoints identified with high and critical vulnerabilities relating to hardware and software that are patched within 30 days

(Data available in FY19)

38%

Percent of participating federal, civilian, executive branch agencies with an active CDM data feed into the DHS managed Federal Dashboard

Target: 50%

0%

Target: 21%

Percent of participating federal, civilian, executive branch agencies for which CDM capabilities to manage user access and privileges to their networks are being monitored on the DHS managed Federal Dashboard

29%

Percent of participating federal, civilian executive branch agencies for which CDM tools to monitor what is happening on their networks have been made available

Target: 95%

25%

Target: 20%

Percent of incidents detected or blocked by EINSTEIN intrusion detection and prevention systems that are attributed to Nation State Activity

33%

Percent of significant (critical and high) vulnerabilities identified through a DHS assessment of a federal agency high value asset that are mitigated within 30 days

Target: 50%

FY2019

Additional information on the performance measure data accuracy are available at: DHS FY17-19 Annual Performance Report Appendix A

Explanation of Results

Performance Measure	Explanation
Percent of significant (critical and high) vulnerabilities identified by DHS cyber hygiene scanning of federal networks that are mitigated within the designated timeline	The number of participating Federal Departments & Agencies increased by 2 over Q1, to a total of 110. Agencies continue to work to increase their capacity to address the most serious vulnerabilities identified by the enhanced visibility from Cyber Hygiene Scanning. Agencies are working to increase their capacity to address vulnerabilities in a timely manner.
Percent of participating federal, civilian executive branch agencies with an active CDM data feed into the DHS managed Federal Dashboard	CDM has established information exchange connections with a total of nine Chief Financial Officer Act agencies. Summary data of approximately 1.2 million endpoints are currently visible on the Federal Dashboard. Results are consistent with the scheduled release of CDM capabilities.
Percent of participating federal, civilian executive branch agencies for which CDM capabilities to manage user access and privileges to their networks are being monitored on the DHS managed Federal Dashboard	The CDM program office is working to assess and determine what data relating to user access and privileges will feed into the Federal Dashboard. Results are consistent with the scheduled release of CDM capabilities.
Percent of participating federal, civilian executive branch agencies for which Continuous Diagnostics and Mitigation (CDM) tools to monitor what is happening on their networks have been made available	The CDM program office continues to deliver capabilities relating to what is happening on agency networks included in the first Dynamic and Evolving Federal Enterprise Network Defense (DEFEND) award. While no additional deliveries were made during Q2, it is consistent with the deployment schedule.
Percent of incidents detected or blocked by EINSTEIN intrusion detection and prevention systems that are attributed to Nation State activity	Of the 96 incidents detected by EINSTEIN intrusion detection and prevention systems, 23 (24%) have been attributed to suspected Nation State activity.
Percent of significant (critical and high) vulnerabilities identified though a DHS assessment of a federal agency high-value asset that are mitigated within 30 days	Eight of a total of 24 critical and high vulnerabilities across six HVAs receiving an assessment were reported as mitigated by the HVA owner within 30 days. As of May 3, 17 of 24 (71%) had been mitigated. Final approval and implementation of BOD 18-02 will provide additional motivation to agencies to mitigate vulnerabilities within the 30 day timeline, but are unlikely that the 50% target for FY18 will be met.

Additional information on the performance measure data accuracy are available at:
DHS FY17-19 Annual Performance Report Appendix A

Contributing Programs & Stakeholders

Contributing Programs

- Cybersecurity & Communications (CS&C), DHS/NPPD
- DHS Office of the Chief Information Security Officer (OCISO)
- Federal Civilian Executive Branch Agencies
- Agency Security/Network Operations Centers (SOC/NOC)

Stakeholders

- Federal Civilian Executive Branch Agencies
- Federal Chief Information Officers (CIOs)
- Federal Chief Information Security Officers (CISOs)
- Office of Management and Budget (OMB)
- Congress
- Government Accountability Office (GAO)
- Agency Inspectors General (IGs)
- The American Public