Agency Priority Goal Action Plan

# Strengthen Federal Cybersecurity

**Goal Leader:**

Matthew Travis, Deputy Under Secretary, National Protection and Programs Directorate

Performance.gov

Fiscal Year 2018, Quarter 3

# 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**

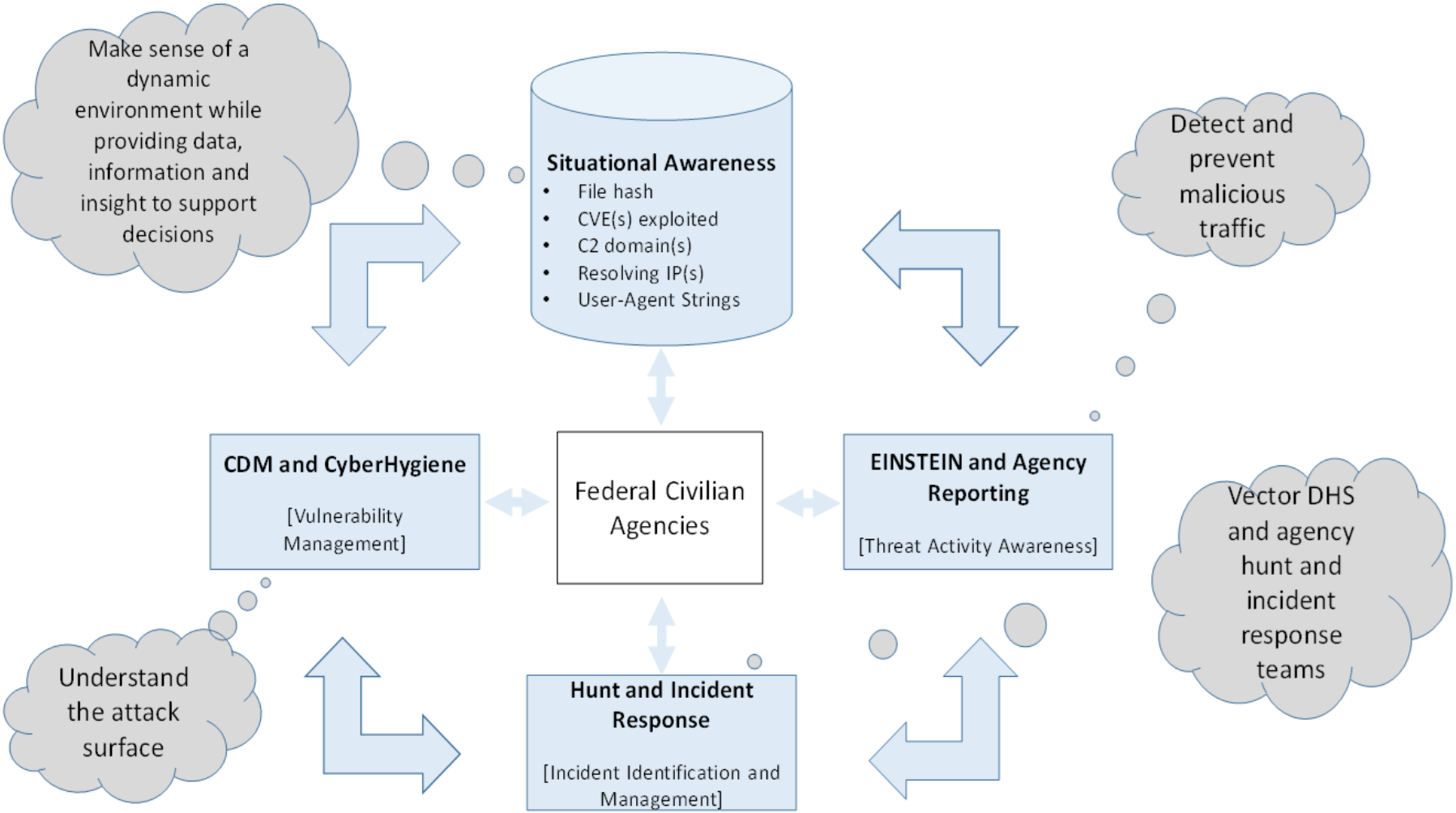
- Continuous scanning, intrusion prevention, and vulnerability assessments allow DHS to provide agencies with the necessary tools and information to take timely and appropriate risk-based actions to defend their networks.
- DHS will continue to engage with senior agency leadership and appropriate information 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

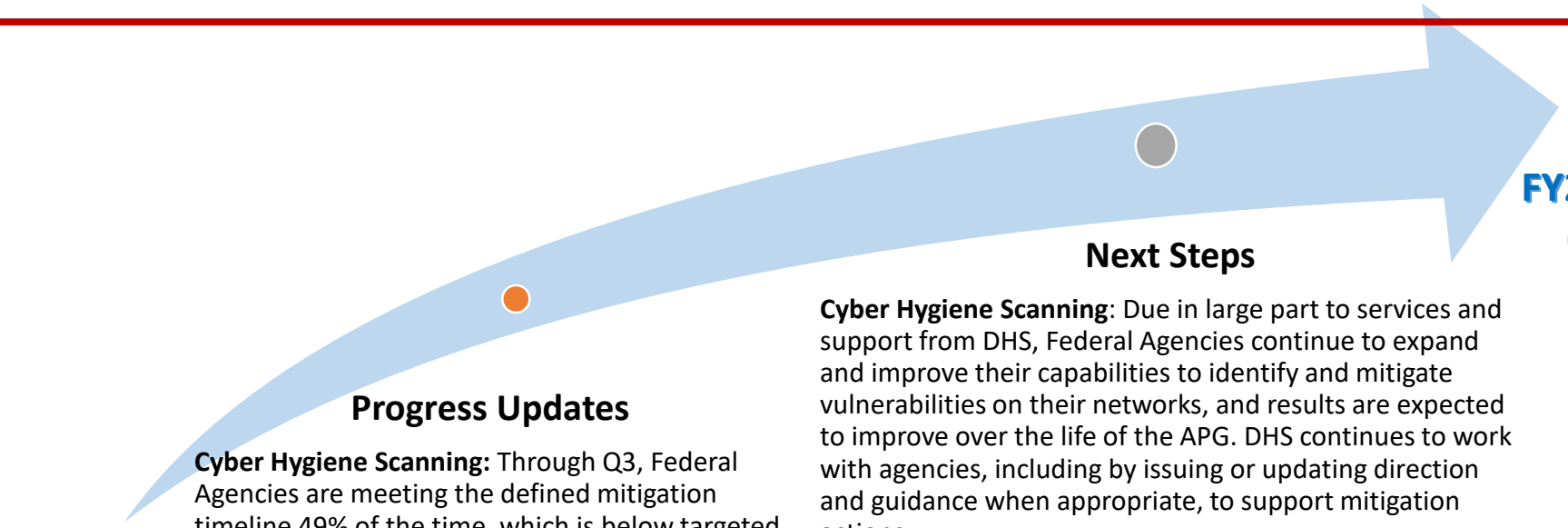
**Strategies:** To effectively strengthen federal network cybersecurity, DHS will coordinate with senior agency leadership to advance agency-level processes and apply the following strategies:

| 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:<br>• Providing an inventory of the hardware and software that is on agency networks.<br>• Providing increased awareness of users on networks to allow agencies to restrict network privileges and access to only those individuals who have a need<br>• 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



# Summary of Progress



**FY2018, Q3**

## Progress Updates

**Cyber Hygiene Scanning:** Through Q3, Federal Agencies are meeting the defined mitigation timeline 49% of the time, which is below targeted levels of performance. NCATS analysts are working to identify the biggest factors affecting vulnerability mitigation in order to make recommendations to the Cyber Hygiene Scanning program and to agencies responsible for mitigation.

**CDM Deployment:** Eleven agencies established a connection with the DHS managed Federal Dashboard in Q3, bringing the total to 20.

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

**FY2018, Q4**

## 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 Management Office is working with agency CIOs and the integrators to identify timelines to complete information exchanges between agency and federal dashboards.

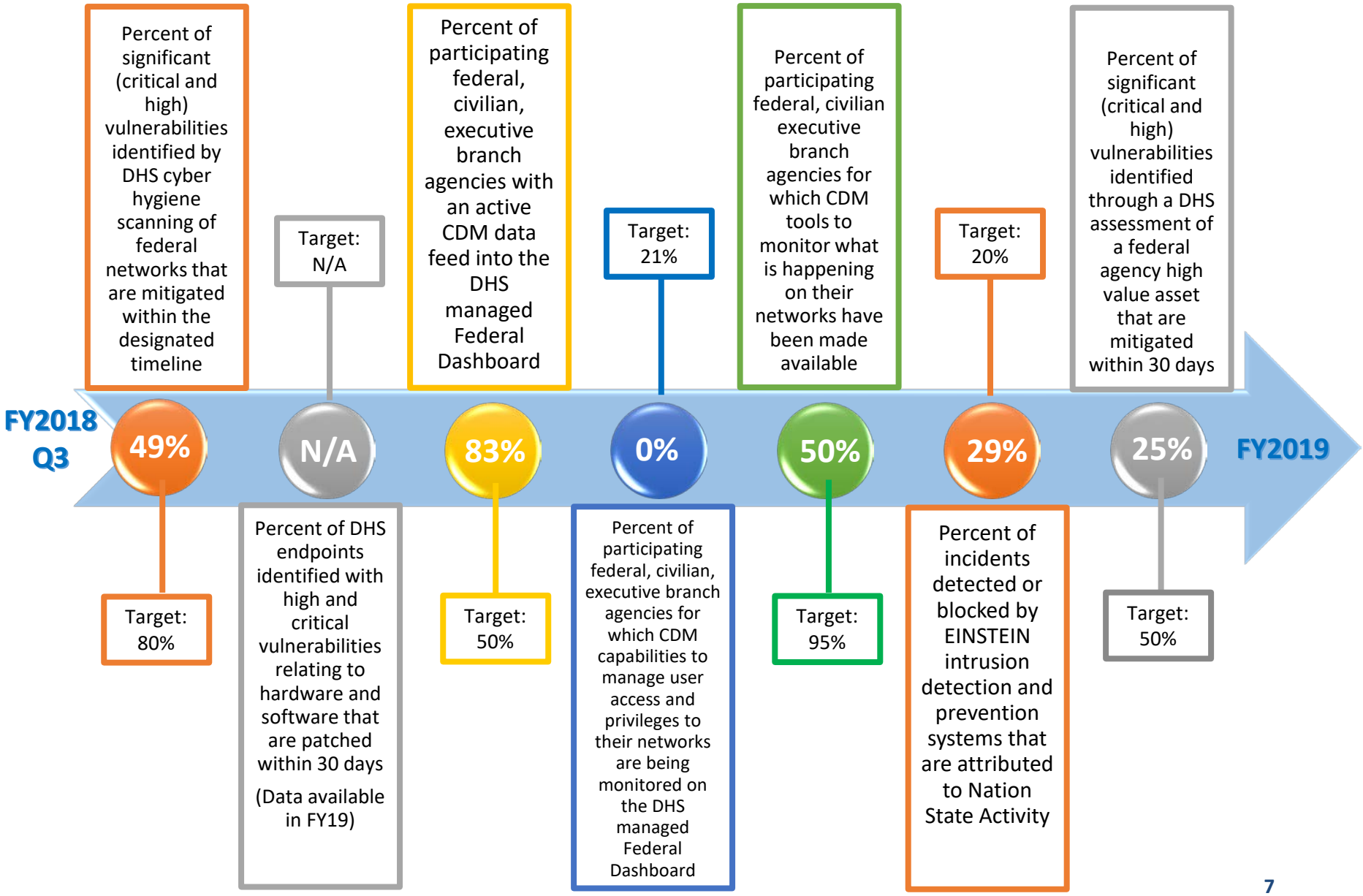
As of early Q4, four non-CFO Act shared-service agencies have integrated capabilities to manage user access and privileges to their network, with full information exchange with enough agencies to meet the target expected in Q4.

**High Value Assets:** Office of Cybersecurity and Communications (CS&C) is developing supplemental guidance to re-affirm, per BOD 18-02, that it is the responsibility of the agency-designated Senior Accountable Official for Risk Management (SAORM) and HVA Point of Contact to coordinate across multiple HVA system owners to remediate and report on vulnerabilities and the need for improvement in this area.

# 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 | Complete | Just past the end of Q3, as of July 12, four non-CFO Act Agencies have initiated Phase 2 information exchange with the Federal Dashboard, with more expected in the coming weeks. CFO Act agencies are expected to begin connections during Q4. |
| Delivery of Phase 3 capabilities (events on Federal networks) completed for participating agencies | Q4, FY18 | In Process | The CDM Project Management Office continues to deploy phase 3 capabilities to agencies included in the DEFEND awards (CDM task order awards administered by GSA). All groups under the DEFEND contract are expected to be awarded by the end of the FY18. |

# Key Indicators



# 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 | When querying the Q3 results, a minor discrepancy was identified in the output that was not as noticeable in pulls for previous quarters. This led the National Cybersecurity Assessment and Technical Services (NCATS) team to review the source data and determine that the previously-reported results did not include some in-scope vulnerabilities. The numbers have been updated, and the analyst team is doing a substantive review of the data to provide a more in-depth analysis of vulnerability mitigation at federal agencies that is difficult to present in a single result. |
| Percent of participating federal, civilian executive branch agencies with an active CDM data feed into the DHS managed Federal Dashboard | Eleven more CFO Act agencies have established data feeds to the Federal Dashboard during Q3, bringing the total up to 20 agencies, or 83%, representing visibility to an additional 1,194,671 endpoints. The 50% target for FY18 has been met. |
| 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 Project Management Office is working with Phase 2 integrators to assess and determine what phase 2 data will feed into the Federal Dashboard. Results are consistent with the scheduled release of CDM capabilities, so the FY18 forecast remains Likely to Meet. (4 non-CFO act shared-service agencies began Phase 2 exchanges in early Q4). |
| 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 Project Management Office continues to deploy phase 3 capabilities to agencies included in the DEFEND awards. Awards for Groups A (DHS), C (5 Agencies), and E (6 Agencies) were made during Q3; however, as of the end of Q3, E is under protest. This brings the total to 12 agencies, or 50%. Assuming the protest is resolved quickly and D is awarded as scheduled in July, the 95% target for FY18 is Likely to Meet. |
| Percent of incidents detected or blocked by EINSTEIN intrusion detection and prevention systems that are attributed to Nation State activity | Of the 52 incidents detected by EINSTEIN intrusion detection and prevention systems in Q3 FY2018, 22 (42%) 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 | Six of 31 (19%) of identified in-scope vulnerabilities were reported mitigated within 30 days. DHS is identifying more enterprise-level vulnerabilities on inter-connected systems to the HVA. The enterprise-level vulnerabilities can create difficult operational and design issues for agencies and may require re-architecting a portion of the network, adding new enterprise-level controls, and/or significant investments in new hardware and/or software. |

# 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