Agency Priority Goal Action Plan

Strengthen Federal Cybersecurity

Goal Leader:

Matthew Travis, Deputy Director, Cybersecurity and Infrastructure Security Agency

Performance.gov

Fiscal Year 2018, Quarter 4

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

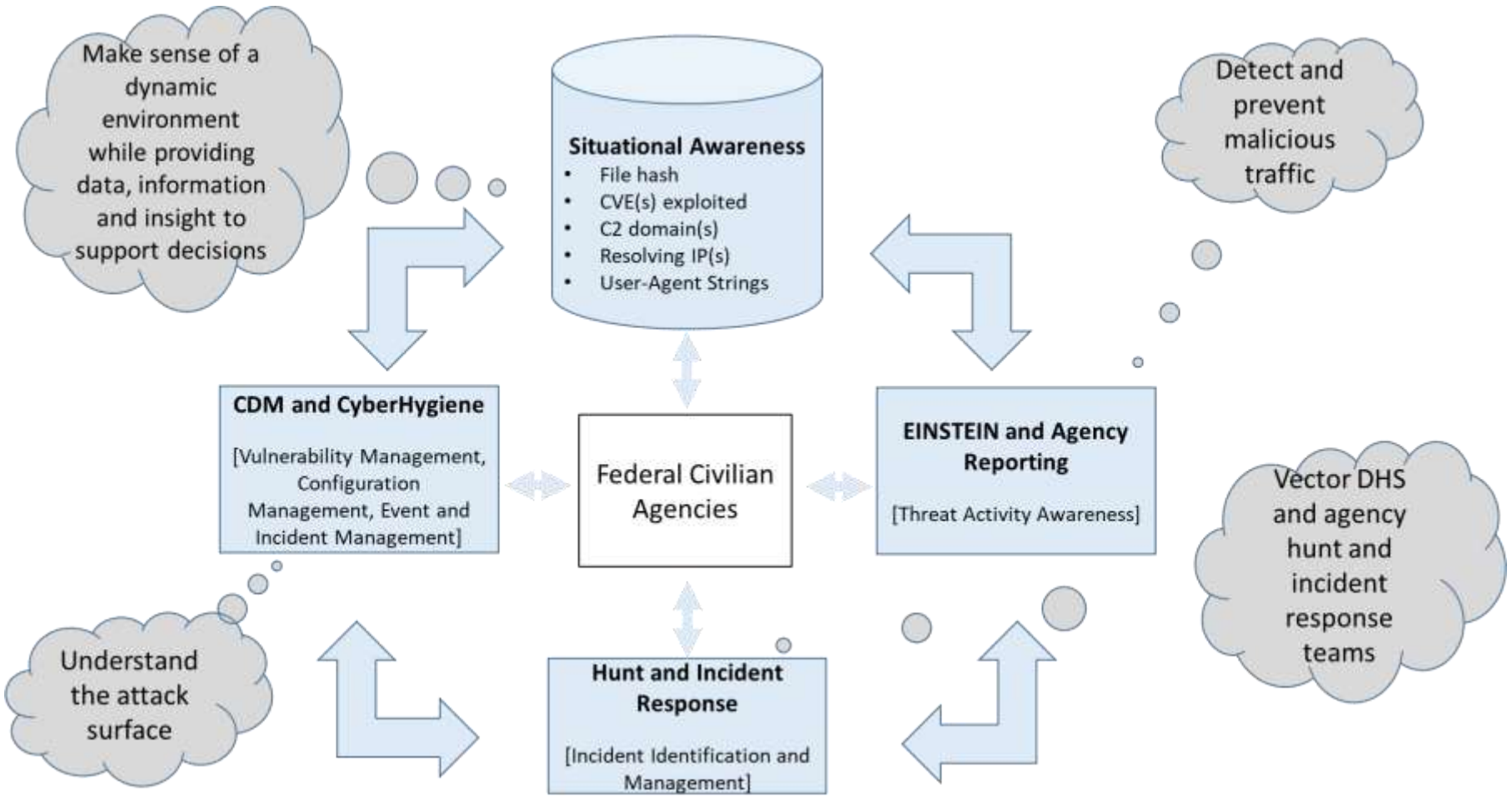
- Continuous scanning, intrusion prevention, and vulnerability assessments allow DHS to provide agencies with the necessary tools and information to take timely and appropriate risk-based actions to defend their networks.
- DHS will continue to engage with senior agency leadership and appropriate information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

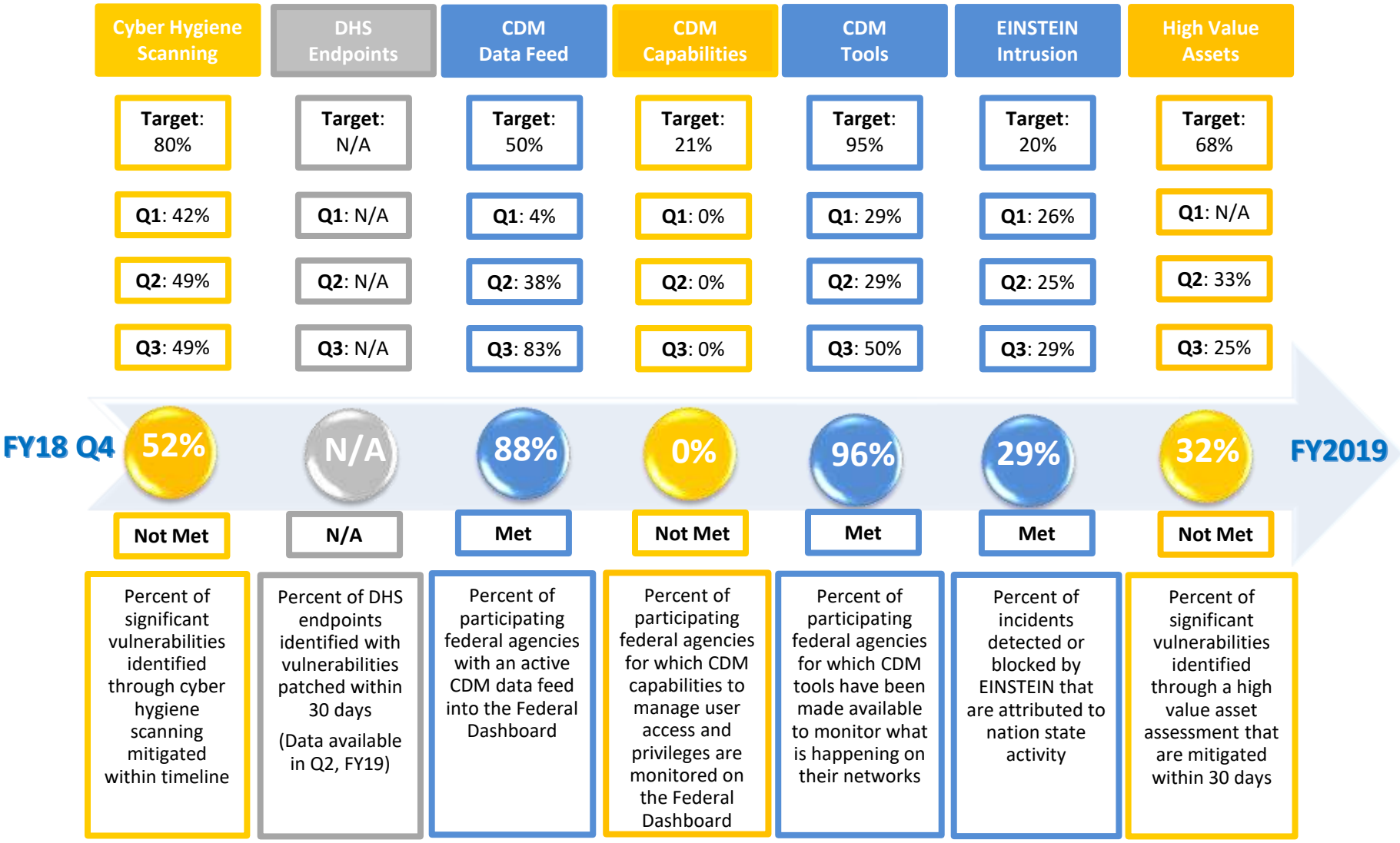
Strategies: To effectively strengthen federal network cybersecurity, DHS will coordinate with senior agency leadership to advance agency-level processes and apply the following strategies:

Cyber Hygiene Scanning	Continuous Diagnostics and Mitigation (CDM)	EINSTEIN	High Value Asset (HVA) Assessments	Hunt & Incident Response Team (HIRT)
Per Binding Operational Directive 10-01, DHS will scan an agency's network for vulnerabilities on its external public-facing assets and connections and will work with that agency to mitigate them effectively.	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 identify or deny access to federal networks by malicious actors 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 and external sources to perform analysis.

Goal Structure & Strategies



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	A key reason this measure did not meet the target is the difference between the required mitigation timeline specified in Binding Operational Directive (BOD) 15-01 and the mitigation timeline defined in the indicator. BOD 15-01 requires agencies to mitigate critical vulnerabilities in 30 days, with no requirement for high vulnerabilities. The definition of the metric calls for a 15-day mitigation timeline for critical vulnerabilities and a 30-day timeline for high vulnerabilities. According to the standard in BOD 15-01, agencies mitigated 79% of critical vulnerabilities on time.
Percent of participating federal civilian executive branch agencies with an active Continuous Diagnostics and Mitigation (CDM) data feed into the DHS-managed Federal Dashboard	One additional CFO Act agency and four non-CFO Act agencies established a validated information exchange with the Federal Dashboard during Q4, extending Federal Dashboard visibility to 21 CFO Act agencies and more than 2.5 million assets across the federal network.
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 protest on the DEFEND E contract was withdrawn, and the contract's kick-off was held in September 2018, but this delayed Group E from establishing Phase 2 (Identity & Access Management) information exchanges with the Federal Dashboard by an estimated six months, a significant factor in not meeting the target. In addition, delays in Groups A-D due to gap-fill activities for Phase 1 (Asset Management) work that was incomplete, along with transition periods between contractors, also contributed to missing the target.
Percent of participating federal civilian executive branch agencies for which CDM tools to monitor what is happening on their networks have been made available	The DEFEND E protest was withdrawn, and the DEFEND E integrator began work in September 2018. This task order covers an additional six CFO Act agencies. Phase 3 (Network Security Management) tools and services are now available to all 23 CFO Act agencies.
Percent of incidents detected or blocked by EINSTEIN intrusion detection and prevention systems that are attributed to nation state activity	The National Cybersecurity and Communications Integration Center (NCCIC) continues to work internally and externally to improve the ability to detect incidents with the EINSTEIN system, through capability development, intelligence, and analysis. In Q4, 26% of detected incidents were attributed to nation states.
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	The accelerated distribution of mitigation guidance and support to participating agencies through individual engagements during and immediately after High Value Asset (HVA) assessments and interagency events spurred an increase in vulnerability mitigations within 30 days during Q4. Also, the type of vulnerabilities identified in Q4 included a higher volume of vulnerabilities typically mitigated within 30 days. About half of the vulnerabilities identified, however, were types that realistically require more than 30 days to mitigate.

Summary of Progress

Cyber Hygiene Scanning

Progress Updates

-The severity level of a particular vulnerability was reevaluated, causing a spike in reporting, which required manual correction of the data.

-Migration of the cyber hygiene scanning capability to a cloud environment caused some initial disruption due to agencies having difficulty recognizing the scans, preventing data from being included in the result. The program is taking steps to mitigate the issue, such as establishing dedicated IP addresses so agencies can easily identify the scanning activity.

Next Steps for FY19

-A revision to BOD 15-01 to address the mitigation timeline requirements is planned, with a proposed draft expected by the end of Q2, FY19.

-CISA staff are working to identify the biggest factors affecting vulnerability mitigation in order to make recommendations to improve the mitigation rate.

CDM Deployment

Progress Updates

-Phase 1 (Asset Management) has completed all but two exchanges for CFO Act agencies, meeting all FY 18 Phase 1 milestones.

-Progress on Phase 2 (Identity & Access Management) exchanges gained momentum with the contract protest withdrawal of the DEFEND E (6 agencies) in Q4.

-Phase 3 (Network Security Management) tools and services are now available to all CFO Act agencies, with only non-CFO Act Phase 3 exchanges remaining.

Next Steps for FY19

-The CDM program office will continue to work with the integrators of all DEFEND groups on Phase 2 exchange timelines.

-Five agencies are expected to complete Phase 2 by Q2, FY19.

-DEFEND F is expected to be awarded in Q3, FY19.

-The measure, "*Percent of DHS endpoints identified with high and critical vulnerabilities relating to hardware and software that are patched within 30 days,"* is estimated to begin reporting in Q2, FY 19.

High Value Assets

Progress Updates

-Federal Network Resilience (FNR) prioritized delivery of guidance to, and direct engagement with, agencies with the largest number of unmitigated vulnerabilities to improve the mitigation rate in Q4.

-FNR also escalated those agencies' mitigation status to their leadership to coordinate an effective response.

Next Steps for FY19

-FNR will continue to support agencies through targeted mitigation guidance and escalation of mitigation priorities to agency leadership.

-Mandatory involvement of agency-designated Senior Accountable Officials for Risk Management (SAORMs), per BOD 18-02, will bring increased visibility, prioritization, and resources to agencies' mitigation efforts.

-FNR is establishing an HVA interagency community of interest (COI) to identify and promote HVA best practices and foster a whole-of-government approach to reducing systemic risk.

Key Milestones-FY18

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 18, CDM has established information exchange connections with a total of nine Chief Financial Officer (CFO) Act agencies.
First exchanges of CDM Phase 2 (Identity & Access Management) information from Agency Dashboards to the Federal Dashboard	Q3, FY18	Complete	Four non-CFO Act agencies initiated Phase 2 (Identity & Access Management) information exchanges with the Federal Dashboard, with more expected in the coming months. CFO Act agencies are expected to begin connections during Q1, FY 19.
Delivery of Phase 3 (Network Security Management) capabilities (events on Federal networks) completed for participating agencies	Q4, FY18	On Track	This milestone is categorized as "on track" but not yet completed. The DEFEND contract actions group agencies by letter. The DEFEND E integrator began work in September 2018, which covers an additional six CFO Act agencies, and most non-CFO agencies are still awaiting Phase 3 capabilities. *Thus this milestone is continued in FY19.*

Key Milestones-FY19

Key Milestone	Milestone Due Date	Milestone Status	Comments
Phase 1 (Asset Management) data exchanges for the remaining CFO Act Agencies complete	Q1, FY19	On Track	Work on the remaining two CFO Act agencies (Department of the Treasury and the Social Security Administration) is ongoing, and they are anticipated to be fully tested and validated by the end of Q1, FY19.
Phase 2 (Identity & Access Management) information exchanges with the Federal Dashboard established for five agencies	Q2, FY19	On Track	The CDM program office is working with the DEFEND E integrator to expedite Phase 2 (Identity & Access Management) information exchanges, as well as with the integrators for DEFEND groups A-D.
Delivery of Phase 3 (Network Security Management) capabilities (events on Federal networks) completed for participating agencies	Q3, FY19	On Track	The DEFEND contract actions group agencies by letter. The DEFEND F action, which covers the majority of non-CFO Act agencies, is expected to be awarded in Spring 2019, to complete the milestone.
Phase 1 (Asset Management) data exchanges for the remaining non-CFO Act Agencies complete	Q4, FY19	Scheduled	DEFEND F, which covers the majority of non-CFO Act agencies, is expected to be awarded in Spring 2019.

Contributing Programs & Stakeholders

Contributing Programs

- Cybersecurity Division (CSD), DHS/CISA
- 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