Agency Priority Goal Action Plan

Strengthen Federal Cybersecurity

Goal Leader:

Matthew Travis, Deputy Director, Cybersecurity and Infrastructure Security Agency

Performance.gov

Fiscal Year 2019, Quarter 2

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 70% 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, 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 augment existing agency capabilities with additional tools and information to assist them in taking 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

Per Binding Operational Directive (BOD) 19-02, DHS will scan an agency's network for vulnerabilities on its Internet-facing assets and connections and will work with that agency to ensure that the agency mitigates them effectively within established timelines.

Continuous Diagnostics and Mitigation (CDM)

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.

EINSTEIN

DHS provides boundary protection to identify or deny access to federal networks by malicious actors through EINSTEIN.

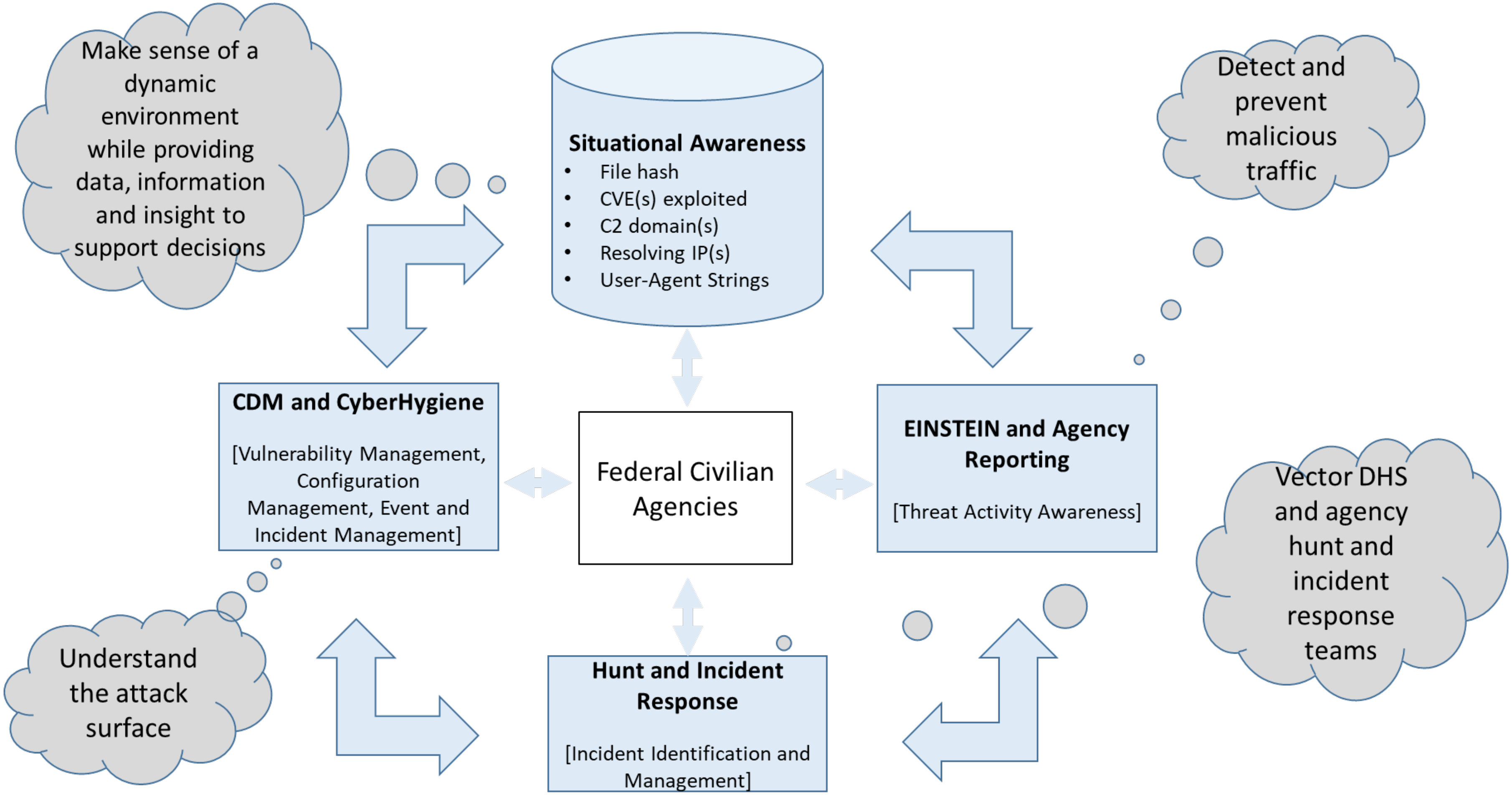
High Value Asset (HVA) Assessments

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.

Hunt & Incident Response Team (HIRT)

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



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, Configuration Management, Event and Incident 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]

Key Indicators

	Cyber Hygiene Scanning	DHS Endpoints	CDM Data Feed	CDM Capabilities	CDM Tools	EINSTEIN Intrusion	High Value Assets	
Target	70%	90%	100%	42%	100%	21%	45%	
Q1	32%	N/A	98%	0%	96%	9%	29%	
FY19 Q2	38%	N/A	98%	9%	96%	14%	33%	FY19 Q3
	Unlikely to Meet	N/A	Likely to Meet	Likely to Meet	Unlikely to Meet	Unlikely to Meet	Unlikely to Meet	
	Percent of significant vulnerabilities identified through cyber hygiene scanning mitigated within timeline	Percent of DHS endpoints identified with vulnerabilities patched within 30 days	Percent of participating federal agencies with an active CDM data feed into the Federal Dashboard	Percent of participating federal agencies for which CDM capabilities to manage user access and privileges are monitored on the Federal Dashboard	Percent of participating federal agencies for which CDM tools have been made available to monitor what is happening on their networks	Percent of incidents detected or blocked by EINSTEIN that are attributed to nation state activity	Percent of significant vulnerabilities identified through a high value asset assessment that are mitigated within 30 days	

Explanation of Results – 1 of 2

Performance Measure	Explanation
Cyber Hygiene Scanning *Q1: 32%* *Q2: 38%* *Target: 70%*	The metric is currently below target due to misalignment with the requirement of agencies in BOD 15-01, which only required agencies to mitigate critical vulnerabilities within 30 days and had no requirement for mitigating high vulnerabilities, and the standard defined in the indicator, which is 15 days to mitigate a critical vulnerability and 30 days to mitigate a high vulnerability. BOD 19-02, which replaces BOD 15-01, was issued on April 29 and contains the same timeline standards as the indicator. Timely vulnerability mitigation in Q2 also was impacted by the partial government shutdown, as multiple agencies contacted CISA to report that those responsible for mitigating vulnerabilities were furloughed.
DHS Endpoints *Q1: N/A* *Q2: N/A* *Target: 90%*	No change from Q1. Due to architectural issues with the agency dashboard, and continued CDM implementation efforts within DHS, the DHS CIO is forecasting that it may not be able to report a result for this measure until FY20. The DHS CIO is forecasting that full CDM program completion of asset management and identity and access management capabilities will occur by the end of FY19. The new CDM dashboard contract (likely to be awarded in Q3) will allow the program to ensure that the architecture supports DHS needs and that high performance is achieved, despite the exponential scale of data collected.
CDM Data Feed *Q1: 98%* *Q2: 98%* *Target: 100%*	No change from Q1. There are still 23 of 23 CFO Act agencies and 16 of 40 non-CFO Act agencies exchanging Asset Management data with the Federal Dashboard.
CDM Capabilities *Q1: 0%* *Q2: 9%* *Target: 42%*	As of the end of Q2, 2 of 23 CFO Act agencies (National Science Foundation and Nuclear Regulatory Commission) have successfully exchanged Identity and Access Management summary data with the Federal Dashboard; eight non-CFO Act agencies from Group F are also exchanging Identity and Access Management data with the Federal Dashboard.

Explanation of Results – 2 of 2

Performance Measure	Explanation
CDM Tools *Q1: 96%* *Q2: 96%* *Target: 100%*	No change from Q1. There are 23 of 23 CFO Act agencies and four non-CFO Act agencies now covered under CDM DEFEND task orders to provide CDM tools and associated services to monitor what is happening on their networks. The DEFEND F task order covering 40-plus non-CFO Act agencies has not been awarded yet. Delays resulting from the partial government shutdown have impacted the pre-solicitation activities, including the release of the request for proposals. As a result, the DEFEND F task order, which covers the remainder of participating non-CFO Act agencies, is expected to be awarded in Q1 FY20.
ENSTEIN Intrusion *Q1: 9%* *Q2: 14%* *Target: 21%*	Since we have no control over how many nation state attacks there may be, it is not possible to control the results of this measure. The NCCIC continues to work internally and externally to improve the ability to detect incidents with the EINSTEIN system through capability development, intelligence, and analysis. Detection is a bigger challenge than attribution.
High Value Assets *Q1: 29%* *Q2: 33%* *Target: 45%*	Performance on this indicator improved over last quarter. In Q2, 3 out of 7 critical and high risks and/or vulnerabilities were mitigated within 30 days; these were configuration-based vulnerabilities that are typically more feasible to address within the 30-day timeline. Two additional configuration-based vulnerabilities were mitigated within 45 and 75 days, respectively. The remaining two vulnerabilities were structural, which typically require a longer mitigation timeline. This measure will continue to have high variance due to the variety and difficulty of vulnerabilities identified each quarter and the different maturity levels of assessed agencies.

Summary of Progress

Cyber Hygiene Scanning

Progress Updates

- Agencies continue to work to increase their capacity to address the most serious vulnerabilities across the board, identified by the enhanced visibility from Cyber Hygiene Scanning, CDM, and internal/external assessments.

Next Steps

- 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. In some instances, substantial investment and time is needed to address significant vulnerabilities. As more CDM vulnerability information becomes available over time, agencies will gain additional insight from inside their networks to compliment the Cyber Hygiene Scanning results.

- BOD 19-02, which updates and replaces BOD 15-01, was issued April 29 and implements stricter timelines to mitigate critical and high vulnerabilities within 15 and 30 days, respectively.

CDM Deployment

Progress Updates

- 2 CFO Act agencies (NSF and NRC) have begun exchanging Identity and Access Management summary data with the Federal Dashboard.

- 8 of 40 non-CFO Act agencies have begun exchanging Identity and Access Management summary data with the Federal Dashboard.

Next Steps

- Efforts continue towards establishment of additional data exchanges between the remaining non-CFO Act agencies and the Federal Dashboard. The program expects to have data exchanges with 30 non-CFO Act agencies by the end of FY 2019.

- The program expects 4 additional CFO Act agencies to begin exchanging user and privileged access summary data with the Federal Dashboard by the end of Q3.

High Value Assets

Progress Updates

- CISA completed Risk and Vulnerability Assessments (RVAs) on six HVAs at two Federal agencies in Q2, fewer than expected due to the partial government shutdown.

Next Steps

- All agencies with open critical and high risks and/or vulnerabilities have mitigation plans in place and continue to make progress. Detailed remediation plans, in addition to established actions and milestones, are now required, and will allow DHS to provide tailored assistance to agencies to mitigate risks and/or vulnerabilities.

- The now mandatory involvement of agency Senior Accountable Officials for Risk Management (SAORM) in FY 19 will elevate HVA risks and/or vulnerabilities to an enterprise-level risk and ensure enterprise-level visibility and allocation of resources for mitigation.

Key Milestones

Key Milestone	Milestone Due Date	Milestone Status	Comments
Phase 1 (Asset Management) data exchanges for the remaining CFO Act Agencies complete	Q1, FY19	Complete	Completed testing on the remaining two CFO Act agencies (Department of the Treasury and the Social Security Administration).
Phase 2 (Identity & Access Management) information exchanges with the Federal Dashboard established for five agencies	Q2, FY19	Missed	The partial government shutdown severely affected the ability to meet this milestone by the end of Q2. Two CFO Act agencies have added Identity and Access Management summary data to agency data feeds, and four more are expected by the end of Q3. The program expects to meet the FY 19 target of ten agencies by the end of the fiscal year.
Delivery of Phase 3 (Network Security Management) capabilities (events on Federal networks) completed for participating agencies	Q3, FY19	On Track	The remaining DEFEND task order to award is for Group F, which covers the majority of non-CFO Act agencies. This award is expected now in Q1 FY20, due to delays in pre-solicitation activities resulting from the partial government shutdown
Phase 1 (Asset Management) data exchanges for the remaining non-CFO Act Agencies complete	Q4, FY19	On Track	Data exchanges for 16 non-CFO Act agencies completed testing by the end of Q1, and efforts continue on completing the remaining non-CFO Act agency data exchanges. The program expects to have a total of 30 non-CFO Act agencies exchanging data by the end of the fiscal year.

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