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 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 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 agencies 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 15-01, DHS will scan an agency's network for vulnerabilities on its public-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.

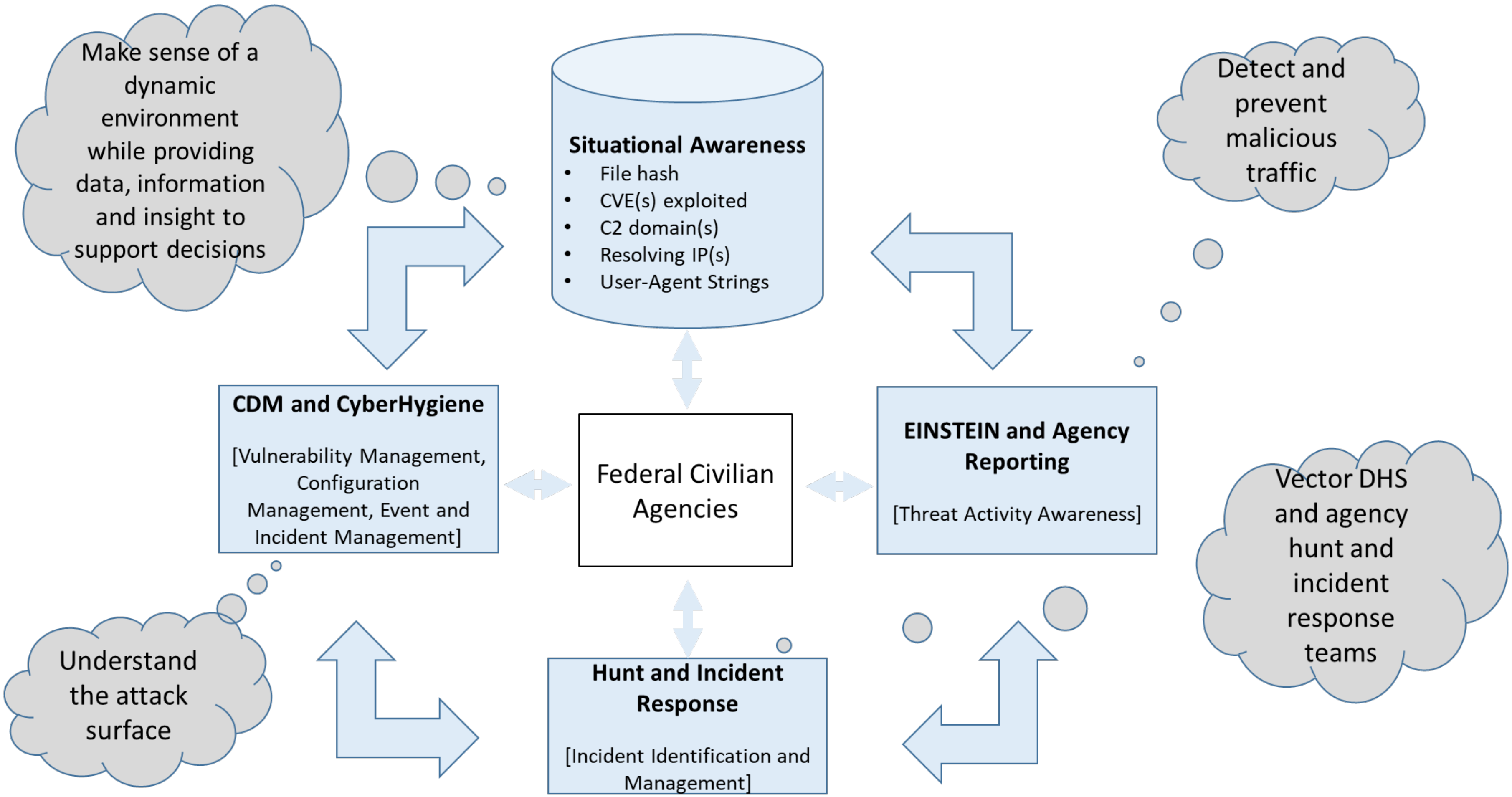
High Value Asset (HVA) Assessments

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%
Q2	38%	N/A	98%	9%	96%	14%	33%
FY19 Q3	50%	77%	98%	22%	96%	16%	32%
	Unlikely to Meet	Unlikely to Meet	Unlikely 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

FY19 Q4

Explanation of Results

Performance Measure	Explanation
Cyber Hygiene Scanning: Percent of significant vulnerabilities identified by DHS cyber hygiene scanning mitigated within the designated timeline Q1: 32% Q2: 38% Q3: 50% Target: 70%	On April 29,2019 DHS released Binding Operational Directive (BOD) 19-02, Vulnerability Remediation Requirements for Internet-Accessible Systems. The purpose of this BOD was to continue to enhance agencies' security posture, reduce risks posed by vulnerable Internet-accessible systems, and build upon the success of BOD 15-01 by advancing federal requirements for high and critical vulnerability remediation to farther reduce the attack surface and risk to federal agency information systems. The new BOD reduces the requirement to mitigate critical vulnerabilities from 30 days to 15 days and to address high vulnerabilities within 30 days. This BOD is intended to drive agencies to meet performance expected for this measure.
DHS Endpoints: Percent of DHS endpoints identified with high and critical vulnerabilities patched within 30 days Q1: N/A Q2: N/A Q3: 77% Target: 90%	Based on the vulnerability scan data collected from all DHS components and reported monthly on the DHS FISMA scorecard , DHS for Q3 is at 77% for this measure. Each month, components use a network scanning tool to collect information about the devices connected to their network. Those scan results are then uploaded, by the component, into the departments asset management tool, where the data is normalized. The data then moves through the Continuous Monitoring Database, to the DHS Information Assurance Repository (DIAR). DAIR applies the calculations detailed in the Information Systems Security Plan, which results in the scores reflected on the Monthly Scorecard.
CDM Data Feed: Percent of federal civilian agencies with an active CDM data feed into the DHS-managed Federal Dashboard Q1: 98% Q2: 98% Q3: 98% Target: 100%	All 23 CFO Act agencies have established data exchanges with the Federal Dashboard. An additional eight non-CFO Act agencies established data exchanges by the end of Q3 FY2019, bringing the overall count up to 22 non-CFO Act agencies exchanging data, but not reaching all non-CFO Act agencies being included in this measure.

Explanation of Results-Continued

Performance Measure	Explanation
CDM Capabilities: Percent of federal civilian agencies for which CDM capabilities to manage user access/ privileges are monitored on the Federal Dashboard Q1: 0% Q2: 9% Q3: 22% Target: 42%	As of Q3 FY2019, five CFO Act agencies (National Science Foundation, Nuclear Regulatory Commission, Environmental Protection Agency, Housing and Urban Development, and U.S. Agency for International Development) and thirteen non-CFO Act agencies have successfully established a data exchange of user access and privileges data with the Federal Dashboard.
CDM Tools: Percent of participating federal civilian executive branch agencies for which CDM tools to monitor what is happening on their networks have been made available Q1: 32% Q2: 38% Q3: 96% Target: 100%	All 23 of the CFO Act agencies are now covered by awarded DEFEND task orders, providing tools to monitor what is happening on their networks. The DEFEND F task order, which will cover the participating non-CFO Act agencies, is projected to be awarded by the end of Q1 FY2020.
ENSTEIN Intrusion: Percent of incidents detected/ blocked by EINSTEIN intrusion detection and prevention systems attributed to nation state activity Q1: 9% Q2: 14% Q3: 16% Target: 21%	These results provide in indicator of the level of nation state activity involved in incidents on federal networks that are detected and blocked by EINSTEIN. DHS 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.

Explanation of Results-Continued

Performance Measure	Explanation
High Value Assets: Percent of significant vulnerabilities identified though a DHS assessment of a federal agency high value asset that are mitigated within 30 days Q1: 29% Q2: 33% Q3: 32% Target: 45%	The results slightly declined for Q3 because nine agencies received Risk and Vulnerability (RVA) assessments in Q3, but three agencies (VA, DOI, and SEC) did not mitigate any of the combined 23 critical and high vulnerabilities identified. The lack of progress from these agencies was due in part to planning and procurement of enterprise wide solutions that takes much longer than 30 days, misinterpreting language in final RVA report, and being assessed for the first time and working through the mitigation process.

Summary of Progress

Cyber Hygiene Scanning

Progress Updates

-BOD 19-02 was officially published on April 29, 2019 and aligns with the required timeframe for mitigating critical and high vulnerabilities with this measure (previously, only critical vulnerabilities needed to be mitigated within 30 days).

Next Steps

-In order to help maximize agencies' ability to meet timelines for remediation of critical and high vulnerabilities per BOD 19-02, CISA sends automated notification emails to federal stakeholders. If any critical or high vulnerabilities were detected on an agency's network for the first time, an email notification is sent to the affected agency within 24 hours. These alerts help bridge the gap between initial detection (when BOD 19-02's clock starts) and agencies' weekly Cyber Hygiene reports, allowing required federal stakeholders to abide by the remediation timelines set forth in BOD 19-02 to look into the vulnerabilities sooner and address them appropriately.

CDM Deployment

Progress Updates

-As of Q3, three additional CFO Act agencies (EPA, HUD, and USAID) have begun exchanging user access and privileges data with the Federal Dashboard, bringing the total to five.

Thirteen of 40 non-CFO Act agencies have established data exchanges for user and privileged access summary data with the Federal Dashboard.

Next Steps

-Efforts continue with 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 FY2019.

The program continues efforts for additional CFO Act agencies to begin exchanging user and privileged access summary data with the Federal Dashboard by the end of FY19

High Value Assets

Progress Updates

-CISA met with agency personnel (CISOs, HVA POCs, and supporting staff) to clarify mitigation scope and reporting requirements.

CISA clarified that enterprise wide solutions are encouraged as a holistic measure, but per BOD 18-02, agencies must first mitigate vulnerabilities associated with the HVA or document compensating controls put in place before proceeding with enterprise-wide solutions

Next Steps

-CISA has updated post-assessment guidance in agency out-briefs and external communications to better clarify mitigation scope. This was also addressed during the HVA Sub-committee meetings and will remain a focus moving forward.

Key Milestones

Key Milestone	Milestone Due Date	Milestone Status	Comments
Delivery of CDM Phase 3 (Network Security Management) capabilities (events on Federal networks) completed for participating agencies	Q3, FY19	Missed	The remaining DEFEND task order to award is for Group F, which covers the majority of non-CFO Act agencies. This award is now expected in Q1 FY20, due to delays in pre-solicitation activities resulting from the partial government shutdown.
Cyber Hygiene Scanning	Q3, FY19	Met	BOD 19-02 was released in Q3 to require more stringent agency timeline requirements to mitigate critical and high vulnerabilities within 15 and 30 days respectively.
CDM Phase 2 (Identity & Access Management) information exchanges with the Federal Dashboard established for five agencies	Q4, FY19	On Track	It is anticipated that an additional five agencies will begin sending Identity and Access Management (IAM) data by the end of FY19 to achieve the annual target of 42% (ten agencies).
CDM Phase 1 (Asset Management) data exchanges for the remaining non-CFO Act Agencies complete	Q4, FY19	Off Track	Data exchanges for 8 non-CFO Act agencies completed testing by the end of Q3, which brings the total number to 22. The program expects to have a total of 30 non-CFO Act agencies (out of a total of 40) exchanging data by the end of the fiscal year.
DHS CIO Reporting	Q4, FY19	On Track	DHS will achieve full operational capability of CDM to provide asset management and identity and access management capabilities to Department information security operations.

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