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 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 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

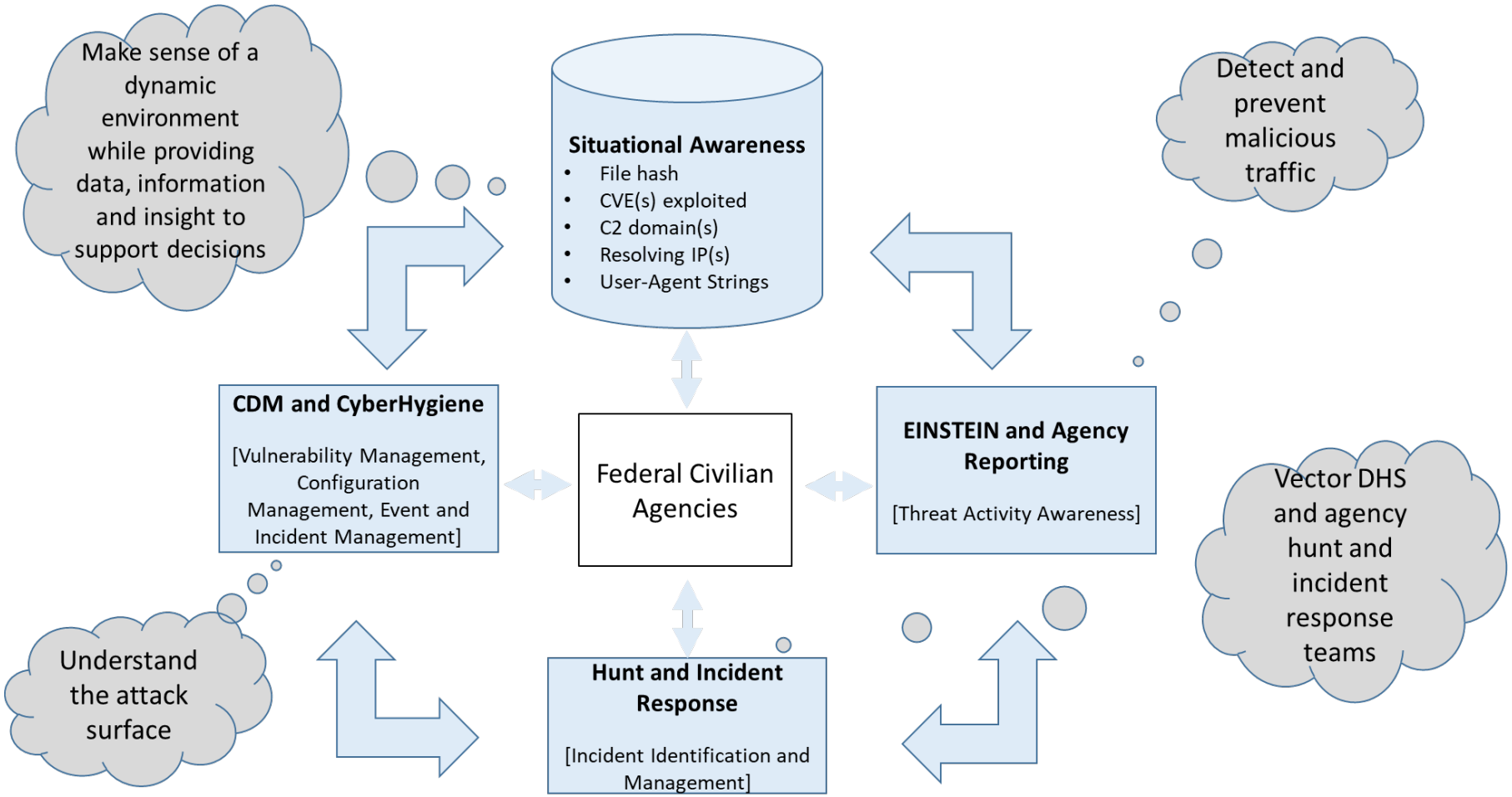
- Continuous scanning, intrusion prevention, and vulnerability assessments allow DHS to augment existing agencies capabilities with additional tools and information to assist them in taking timely and appropriate risk-based actions to defend their networks.
- DHS will continue to engage with senior agency 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 (1 of 2)

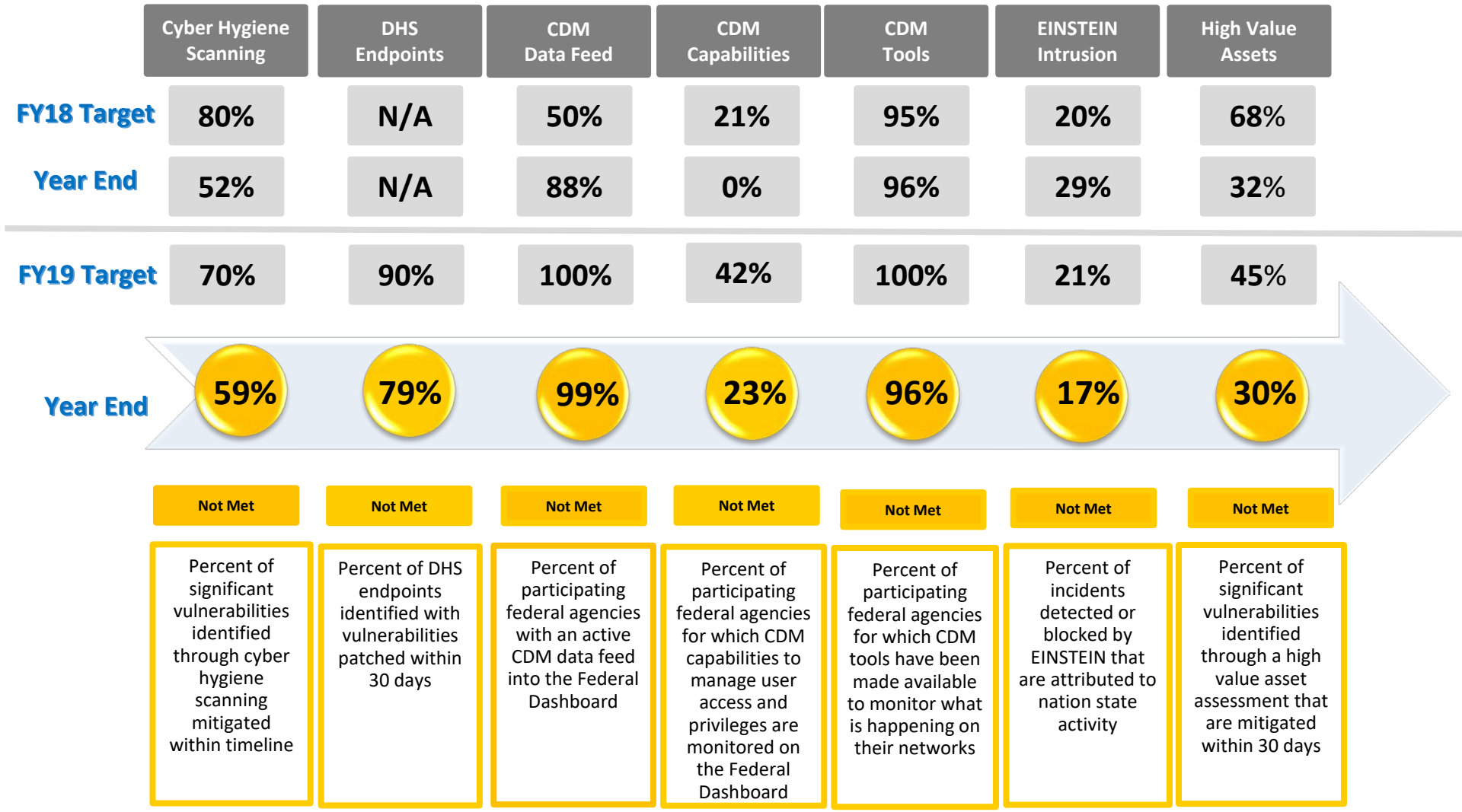
Strategies: To effectively strengthen federal network cybersecurity, DHS will coordinate with senior agency leadership to advance agency-level processes and apply the following strategies:

Cyber Hygiene Scanning	Continuous Diagnostics and Mitigation (CDM)	EINSTEIN	High Value Asset (HVA) Assessments	Hunt & Incident Response Team (HIRT)
Per Binding Operational Directive 19-02, 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.	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 (2 of 2)



Key Indicators



Explanation of Results (1 of 3)

Performance Measure	Explanation
Cyber Hygiene Scanning: Percent of significant vulnerabilities identified by DHS cyber hygiene scanning mitigated within the designated timeline FY18 Target: 80% FY18 Result: 52% FY19 Target: 70% FY19 Result: 59%	During the first half of the year, Binding Operational Directive (BOD) 15-01 was still in place, and the mitigation timelines were not aligned with the standards for this measure. The issuance of BOD 19-02 on April 29 formally established updated mitigation timelines of 15 days for critical vulnerabilities and 30 days for high vulnerabilities. Since BOD 19-02's implementation, the compliance rate has increased substantially, and DHS expects performance to continue to improve in FY20.
DHS Endpoints: Percent of DHS endpoints identified with high and critical vulnerabilities patched within 30 days FY18 Target: N/A FY18 Result: N/A FY19 Target: 90% FY19 Result: 79%	Vulnerability scan data is collected from all DHS components and reported monthly on the DHS FISMA. 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 department's asset management tool, where the data is normalized. The data then moves through the Continuous Monitoring Database, to the DHS Information Assurance Repository (DIAR). DIAR applies the calculations detailed in the Information Systems Security Plan, which results in the scores reflected on the Monthly Scorecard. Note: Vulnerability patch details are unavailable for USCIS for August and September due to Tenable/Nessus issues within USCIS.
CDM Data Feed: Percent of federal civilian agencies with an active CDM data feed into the DHS-managed Federal Dashboard FY18 Target: 50% FY18 Result: 88% FY19 Target: 100% FY19 Result: 99%	CDM has worked with the federal civilian executive agencies to establish data exchanges between agency CDM dashboards and the Federal Dashboard. CDM integrators must work within a number of constraints to complete the installation and configuration of CDM tools, including limited agency resources, competing agency priorities, and ongoing agency operations. As of end of FY19, all 23 civilian CFO-Act agencies and 29 of 40 non-CFO Act agencies have successfully established this data exchange.

Explanation of Results (2 of 3)

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 FY18 Target: 21% FY18 Result: 0% FY19 Target: 42% FY19 Result: 23%	As of end of FY19, 5 of 23 civilian CFO Act agencies and 29 of 40 non-CFO Act agencies have established data exchanges for user access 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 FY18 Target: 95% FY18 Result: 96% FY19 Target: 100% FY19 Result: 96%	The new DEFEND task orders for the 23 civilian CFO Act agencies were awarded in FY18 and are now underway. The final DEFEND F task order for the approximately 40 non-CFO Act agencies was delayed, but is expected to be awarded in early FY20. DEFEND F experienced some delays in the pre-solicitation phase, including scope adjustments requiring a brand name justification, technical considerations for the existing solution, and additional meetings with the current solution provider and the contracting office. There were also additional delays related to the establishment of an electronic reading room to provide offerors with pertinent information relative to the current solution and other CDM guidance documents. These unforeseen delays were due to concerns surrounding data rights of documentation that is targeted for publication in the electronic reading room.

Explanation of Results (3 of 3)

Performance Measure	Explanation
ENSTEIN Intrusion: Percent of incidents detected/ blocked by EINSTEIN intrusion detection and prevention systems attributed to nation state activity FY18 Target: 20% FY18 Result: 29% FY19 Target: 21% FY19 Result: 17%	DHS worked consistently to improve the ability to detect incidents with the EINSTEIN system through capability development, intelligence, and analysis during FY19. Though DHS has no control over how many nation state attacks that occur, detection is the higher priority rather than attribution.
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 FY18 Target: 68% FY18 Result: 32% FY19 Target: 45% FY19 Result: 30%	This metric experienced considerable variance during FY19 due to the variety and difficulty of vulnerabilities identified each quarter and the different maturity levels of assessed agencies. Some agencies did not mitigate all vulnerabilities within 30 days because they elected to implement DHS' recommended mitigation approach across their entire enterprise, rather than apply it only to the High Value Asset (HVA). While DHS supports this more widespread application, it recommends that an agency mitigate the issue within the HVA, specifically, first, as the broader implementation can delay the overall mitigation effort. To further help agencies reduce risks, CISA is establishing methodologies to identify common risks and trends so that solutions and services can be developed to help agencies address their issues more quickly. The solutions may include engineer support, cyberstats, technical engagements, CDM offerings, implementation whitepapers, and governance frameworks.

Summary of Progress

- Over the past two years, agencies have made substantial progress on addressing critical and high vulnerabilities identified during cyber hygiene scanning within required timelines. Timely mitigation has further accelerated following the issuance of BOD 19-02, and additional improvement is expected in FY20.

- CDM has made considerable progress towards delivery of continuous monitoring capabilities across the federal civilian executive branch. The program faced numerous challenges, including: agency ability to provide an accurate count and configuration of assets to be covered; readiness of agencies to support deployment and configuration of CDM tools, and agency ability to balance resource commitments (people, time, assets) with competing mission requirements.

- The CDM portfolio team implemented a more deliberate methodology for CDM tool deployments and integration based on the lessons learned from the initial deployments of Asset Management and Identity & Access Management, which includes close collaboration with agency Chief Information Officer staffs, regular quarterly progress updates with the inter-agency CDM Customer Advisory Forum (CAF), and frequent information exchanges with the Office of Management and Budget (OMB).

- The CDM program will continue to focus on the transition from CDM tool delivery to operationalization, demonstrating the value that CDM contributes through the ability of agencies to identify and prioritize risk and manage endpoints and users.

Key Milestones

Key Milestone	Due Date	Status
First information exchange from an Agency Dashboard to Federal Dashboard	Q1, FY18	Complete
Eight additional information exchanges between Agency Dashboards and the Federal Dashboard	Q2, FY18	Complete
First exchanges of CDM Phase 2 information (user access and privileges) from Agency Dashboards to the Federal Dashboard	Q3, FY18	Missed
Delivery of Phase 3 capabilities (events on Federal networks) completed for participating agencies	Q3, FY19	Missed
CDM Phase 1 (Asset Management) data exchanges for the remaining CFO Act Agencies complete	Q1, FY19	Complete
CDM Phase 2 (Identity & Access Management) information exchanges with the Federal Dashboard established for five agencies	Q4, FY19	Missed
Binding Operational Directive 19-02: *DHS Vulnerability Remediation Requirements* released to require more stringent agency timeline requirements to mitigate critical and high vulnerabilities within 15 and 30 days respectively	Q3, FY19	Complete
CDM Phase 1 (Asset Management) data exchanges for the remaining non-CFO Act Agencies complete	Q4, FY19	Missed
DHS CIO Reporting begins	Q4, FY19	Missed

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