Strengthen Federal Cybersecurity

Goal Lead: Jeanette Manfra, Assistant Secretary for Cybersecurity and Communications

Theme: National Defense

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.
- **Challenges**
  - The cybersecurity threat to federal networks continues to grow and evolve at an alarming rate. Adversaries in cyberspace conduct attacks against federal networks in near real time and collect sensitive data and information in a matter of minutes. Data breaches at the Office of Personnel Management (OPM) and the Internal Revenue Service (IRS) has exposed the data and information of millions of Americans to criminal organizations and hostile nation states. Protecting the personally identifiable information of the American people and other sensitive information pertaining to national security is critical to the Federal government maintaining the trust and confidence of the American public.
  - DHS alone cannot secure the computer networks of federal agencies. The challenge moving forward will be to enable agency use of DHS provided tools and information to take action with the same speed and agility as our adversaries. 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. Leadership engagement and prioritization of cybersecurity across the federal government will be critical to agencies using vulnerability and threat information DHS shares with them to take timely and risk based actions regarding their network security.

Overview (cont.)

- **Opportunity**

  - The array of cybersecurity programs that DHS offers to agencies will enable DHS and agencies to have increased situational awareness of the cybersecurity posture of their networks. Through continuous scanning, intrusion prevention, and vulnerability assessments DHS will provide agencies with the necessary tools and information to take timely and appropriate risk based actions to defend their networks. This will allow agencies to move with comparable speed and agility as our adversaries and increase the time and cost to conduct successful attacks. To ensure the successful implementation and use of these capabilities, DHS will continue to engage with senior agency leadership and appropriate information technology and security experts to apply these programs into agency cybersecurity practices.

  - The deployment of Continuous Diagnostics and Mitigation (CDM) capabilities onto agency networks is a critical step towards increased situational awareness of what assets, people and events are operating on a network. CDM is designed to provide capabilities incrementally to provide agencies with increased information on the security posture of their networks to aid in risk based decision making. Initially an agency must know what hardware and software is on its network before it can take steps to defend it. The capability to monitor user access and events on a network will be implemented in the near future.

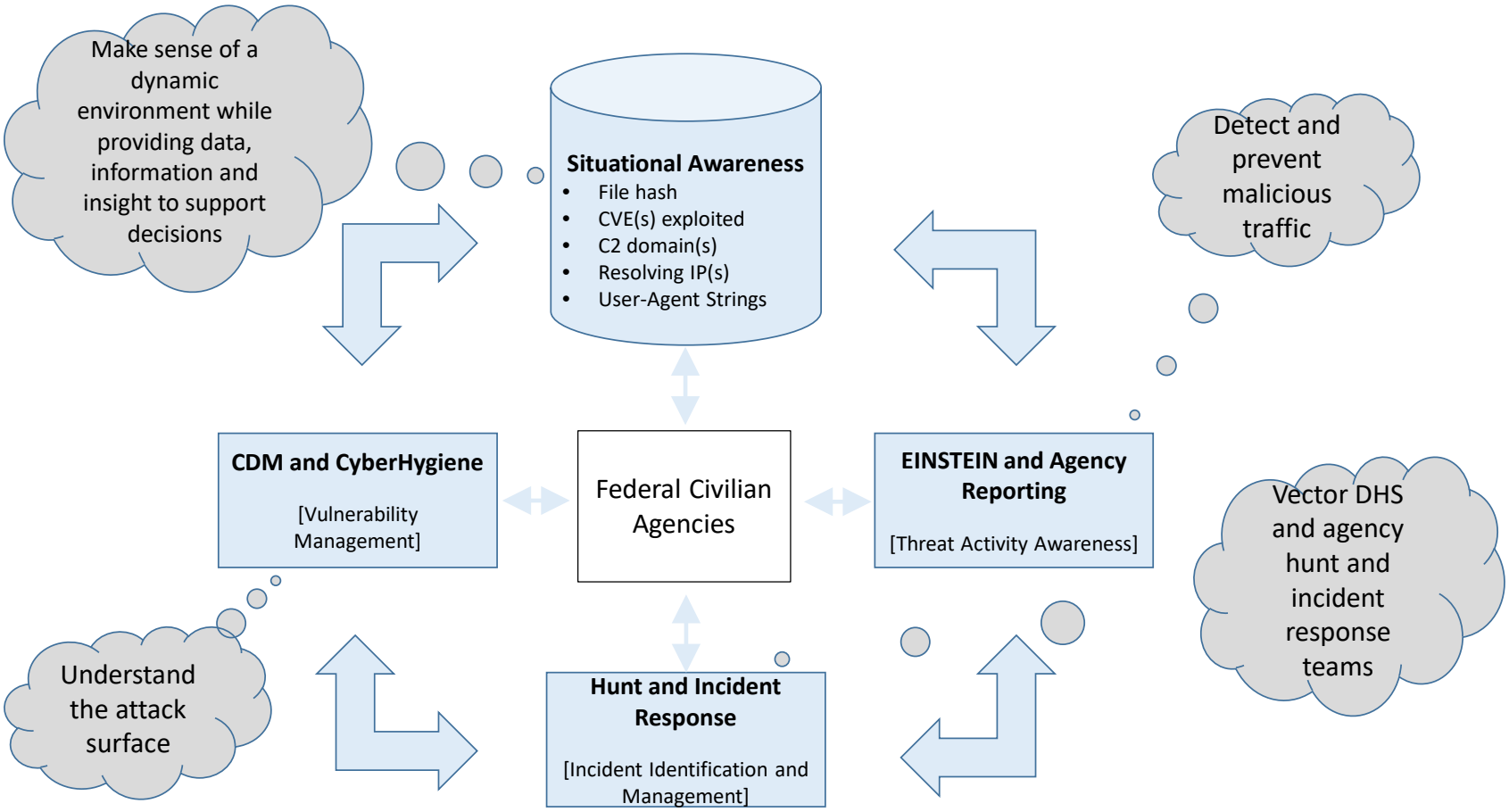
Overview (cont.)

- **Opportunity (cont.)**
  - DHS has focused significant leadership attention and investment towards the deployment of cybersecurity programs to defend the federal network. The transition of technology and tools to participating agencies will continue to be a leadership priority to ensure a smooth transition from acquisition into network security operations. The implementation of these programs is now at a maturity level within Federal agencies to permit the measurement of outcomes related to agency use of the information DHS provides to take actions to secure their networks. This will enable DHS to better manage its cybersecurity programs to increase value and performance delivered to its federal customers.

Goal Structure and Strategies

- To effectively strengthen federal network cybersecurity DHS must coordinate with senior agency leadership, to include Deputy Secretaries, Chief Information Officers, and Chief Information Security Officers, to advance agency-level processes related to their ability to implement and effectively apply DHS provided programs. In order for federal network security to improve, agency senior leadership must make it a priority, and agency staff and leadership responsible for network security must effectively implement and use the tools and information that DHS provides. The 23 civilian CFO Act agencies and additional mid to small sized agencies are the target population for DHS programs to strengthen federal cybersecurity.
- DHS is currently employing tools to enable agencies to implement a defense in depth strategy to defend their networks. Through cyber hygiene scanning, the deployment of CDM, the boundary protection provided by EINSTEIN, and assessments of high value assets DHS will increase the amount and quality of threat and vulnerability information shared with federal agencies. This more holistic assessment of agency network vulnerabilities and threats will enable risk-based decision making to further harden network defenses to increase the time and resources adversaries must invest in cyber attacks.

Goal Structure and Strategies (cont.)



Goal Structure and Strategies (cont.)

- The key indicator of success will be the speed with which agencies mitigate significant vulnerabilities on their respective networks. DHS will employ the following strategies to provide agencies with the tools and information to effectively defend their networks:
  - **Cyber Hygiene Scanning:** Federal civilian executive branch agencies are required to provide DHS with a list of all public facing networks to receive cyber hygiene scanning to identify vulnerabilities. Cyber hygiene scanning is limited to monitoring for vulnerabilities on external facing network connections to agency networks. For a specified time period, DHS will scan an agency network for vulnerabilities on its public facing assets and connections and will work with that agency to effectively mitigate them. Continuous Diagnostics and Mitigation (CDM) is different from cyber hygiene scanning in that it is a maturation from a temporary scanning capability of public facing network assets and connections, to a comprehensive and continuous capability that scans for vulnerabilities relating to assets, users, and events both internal and external to a network.
  - **Continuous Diagnostics and Mitigation (CDM):** CDM will provide agencies with increased awareness of assets, users, and events on their networks. The initial capability that CDM will provide will be an inventory of the hardware and software that is on agency networks. This is a critical first step because an agency must know what assets are on its network before it can take effective action to secure it. This capability will be fully implemented at participating agencies by the end of 2019. The second capability that CDM will provide will be increased awareness of users on networks to allow agencies to restrict network privileges and access to only those individuals who need it to perform their duties. This capability will be implemented at less than half of participating agencies by the end of 2019. The final capability will provide insight into what is happening on an agency network. This phase will provide boundary protection and tools to enable agencies to better understand and manage activity on their networks. The contracts to deliver this capability will be awarded by the end of 2019.

Goal Structure and Strategies (cont.)

- **EINSTEIN:** DHS provides boundary protection to deny entry of malicious activity and actors onto federal networks through EINSTEIN. DHS will focus on providing agencies with indicators of known Nation State activity in order to deny entry of the most sophisticated and persistent cyber threats. Nation States possess expertise and resources that can be sustained over long periods of time that criminal organizations and individual hackers lack. Thus DHS must focus on denying this threat from entering federal networks. To enhance intrusion detection and prevention, DHS is piloting a program to detect and prevent previously unknown threats from entering federal networks. This capability will identify abnormal network behavior and notify agency network security personnel to take appropriate action. The ability to identify and block previously unknown cyber threats and activity will continue to increase the time and resources our adversaries must expend to conduct successful cyber attacks.

Goal Structure and Strategies (cont.)

- **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. HVAs contain the most sensitive data and information on agency networks and thus must be a focus of DHS attention and resources. The result of DHS-led HVA assessments will be actionable information for agencies to use to continue to harden security measures around these sensitive assets.
- **Hunt and 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. The HIRT team utilizes cross-cutting information available from CDM, EINSTEIN, cyber hygiene scanning, and other internal/external sources to perform analysis to determine if a breach has occurred and assist agencies in mitigating root cause vulnerabilities and restoring services.

Contributing Programs

- **Cybersecurity & Communications (CS&C), DHS/NPPD:** CS&C administers the Continuous Diagnostics and Monitoring (CDM) and EINSTEIN programs that provide the technological foundation that enables DHS to secure and defend the federal civilian government's information technology infrastructure against advanced cyber threats. Additionally CS&C coordinates with federal partners to employ DHS cyber security tools and provides both assessments of identified high value assets on stakeholders' networks and response capability to suspected and actual cyber incidents.
- **DHS Office of the Chief Information Security Officer (OCISO):** The DHS OCISO develops, and manages IT security programs, policies, and processes for DHS IT networks. DHS was the first agency to receive and implement CDM tools to monitor its network.
- **Federal Civilian Executive Branch Agencies:** The 23 non-defense CFO Act agencies and additional non-CFO Act agencies that integrate and deploy the DHS delivered cybersecurity programs and assessment information on their respective networks.
- **Agency Security/Network Operations Centers (SOC/NOC):** Agency SOC/NOCs monitor the security of their networks and take appropriate actions based on the information they receive from both their own internal tools and those provided by DHS. The agency SOC/NOCs deploy solutions based on available information to address the most significant vulnerabilities and threats in a timely manner.

Stakeholders

- **Federal Civilian Executive Branch Agencies:** Federal agencies deploy DHS provided tools and take risk based action based on information provided by those tools.
- **Federal Chief Information Officers (CIOs):** Federal CIOs are responsible for the management and oversight of their respective agency's information technology to include security tools provided by DHS.
- **Federal Chief Information Security Officers (CISOs):** Federal CISOs are responsible for implementing and applying DHS provided tools into their agency-wide information security program.
- **Office of Management and Budget (OMB):** OMB is responsible for overseeing federal information-security policy, evaluating agency information-security programs, and promulgating cybersecurity standards.
- **Congress:** Congress provides oversight to ensure that the Executive branch is carrying out federal law pertaining to cybersecurity in a way that Congress intended.
- **Government Accountability Office (GAO):** The GAO engages in oversight of agency activities pertaining to cybersecurity. Their evaluations and analysis are intended to improve performance pertaining to federal network security.
- **Agency Inspectors General (IGs):** IGs perform oversight of cybersecurity programs within their respective agencies. The investigations and reports that IGs produce are intended to improve agency performance and accountability of their cybersecurity programs.
- **The American Public:** The American Public entrusts the Federal government to secure sensitive information that pertains to their own personally identifiable information and national security. Continued data breaches will continue to erode public confidence in the Federal government.

External Communications Plan

- DHS senior leadership will review the performance results of the cybersecurity tools it provides agencies on a quarterly basis to determine progress and any necessary corrective action to be taken by DHS.
- The performance results will also be shared with OMB to highlight areas where their assistance is needed in enabling agencies to build the capacity and government-wide governance structures to effectively implement and use DHS-supplied tools.

Performance Measures

Key Measure

Measure Name: Percent of significant (critical and high) vulnerabilities identified by DHS cyber hygiene scanning of federal networks that are mitigated within the designated timeline	
FY18: 80%	**FY19**: 90%

Measure Description: This measure calculates the percent of significant (critical and high) vulnerabilities identified through cyber hygiene scanning that are mitigated within the specified timeline. For critical vulnerabilities the timeline is 15 days and for high vulnerabilities the timeline is 30 days. DHS provides cyber hygiene scanning to agencies to aid in identifying and prioritizing vulnerabilities based on their severity for agencies to make risk based decisions regarding their network security. Identifying and mitigating the most serious vulnerabilities on a network in a timely manner is a critical component of an effective cybersecurity program.

Performance Measures

Supporting Measure

Measure Name: Percent of DHS endpoints identified with high and critical vulnerabilities relating to hardware and software that are patched within 30 days	
FY18: N/A	**FY19**: 90%

Measure Description: This measure assesses how effectively the Information Technology (IT) operations teams within DHS are able to remediate high and critical risk vulnerabilities identified through the Continuous Diagnostics and Mitigation (CDM) program on the DHS network. The vulnerabilities identified in this measure relate to "What is on the network" in terms of hardware and software. The CDM tool set provides near real time Security IT vulnerability details to DHS officials. By quickly addressing these vulnerabilities, DHS will close security gaps to provide greater protection of its critical IT infrastructure. DHS was the first agency to receive CDM and it is anticipated that the initial tools to monitor endpoints on the DHS network will be fully implemented across the Department by October 2018. The implementation of these tools will enable DHS to measure the speed in which critical and high vulnerabilities are mitigated.

Performance Measures

Supporting Measure

Measure Name: Percent of participating federal, civilian executive branch agencies with an active Continuous Diagnostics and Mitigation (CDM) data feed into the DHS managed Federal Dashboard	
FY18: 50%	**FY19**: 100%

Measure Description: This measure calculates the percent of participating federal, civilian executive branch agencies with an active Continuous Diagnostics and Mitigation (CDM) data exchange with the DHS managed CDM Federal Dashboard. These exchanges demonstrate the successful deployment, integration, display, and exchange of data pertaining to CDM for agencies on Agency Dashboards and summary information at the Federal Dashboard. For a data feed to be established to successfully share information, the infrastructure to do so must first be in place between the agency and DHS. Deploying CDM and establishing data feeds between DHS and Federal agencies will enable greater visibility and management of the vulnerability and security status of Federal IT networks.

Performance Measures

Supporting Measure

Measure Name: Percent of participating federal, civilian executive branch agencies for which Continuous Diagnostics and Mitigation (CDM) capabilities to manage user access and privileges to their networks are being monitored on the DHS managed Federal Dashboard	
FY18: 21%	**FY19**: 42%

Measure Description: This measure calculates the percent of participating federal, civilian executive branch agencies in the Continuous Diagnostics and Mitigation (CDM) program whose data relating to user activities on their network is visible on the DHS managed Federal Dashboard. The data pertaining to "Who is on the Network" demonstrates the successful deployment, integration, display and exchange of data pertaining to this particular CDM capability that focuses on restricting network privileges and access to only those individuals who need it to perform their duties. The data that is visible to the agencies is at the individual/object level while the Federal Dashboard will provide DHS with summary level vulnerability and security information. Deploying CDM and sharing information with Federal agencies will enable greater DHS visibility and management of the security of Federal IT networks.

Performance Measures

Supporting Measure

Measure Name: 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	
FY18: 95%	**FY19**: 100%

Measure Description: This performance measure assesses the extent to which DHS has contractually made available Continuous Diagnostics and Mitigation (CDM) tools to monitor events on their networks to participating federal civilian executive branch agencies. Once DHS has made the tools available through contract award, agencies must still take action to deploy and operate CDM on their networks. By making CDM tools available to agencies, they will be able to more effectively manage coordinated threats to their network.

Performance Measures

Supporting Measure

Measure Name: Percent of incidents detected or blocked by EINSTEIN intrusion detection and prevention systems that are attributed to Nation State activity	
FY18: 20%	**FY19**: 21%

Measure Description: This measure demonstrates the EINSTEIN intrusion detection and prevention systems' ability to detect and block the most significant malicious cyber activity by Nation States on Federal civilian networks. Nation States possess the resources and expertise to not only develop sophisticated cyber attacks but sustain them over long periods of time. Thus the indicators that EINSTEIN deploys to detect and block malicious cyber activity should focus on methods and tactics employed by Nation States. The overall percentage of incidents related to Nation State activity is expected to increase through greater information sharing with partners and improved indicator development, which will result in better incident attribution.

Performance Measures

Supporting Measure

Measure Name: Percent of significant vulnerabilities (critical and high) mitigated within 6 months following a DHS assessment of a Federal Agency high-value asset	
FY18: 68%	**FY19**: 73%

Measure Description: This measure calculates the percentage of significant vulnerabilities (critical and high) identified during a Risk and Vulnerability Assessment (RVA) of a High Value Asset (HVA) that the receiving agency has mitigated within six months of the final report being submitted to the agency to conclude the assessment. RVAs are performed on identified HVAs across the federal government to identify vulnerabilities associated with the federal government's most sensitive IT systems and data. As part of the assessment, the HVA owner agency receives a list of critical and high vulnerabilities to remediate and agencies provide monthly updates on progress. As agency vulnerability mitigation processes improve, more vulnerabilities should be mitigated in shorter time. Mitigating significant vulnerabilities relating to the Federal Government's most sensitive data and systems is critical to preventing potential cyber incidents.

Homeland Security