NPPD AT A GLANCE

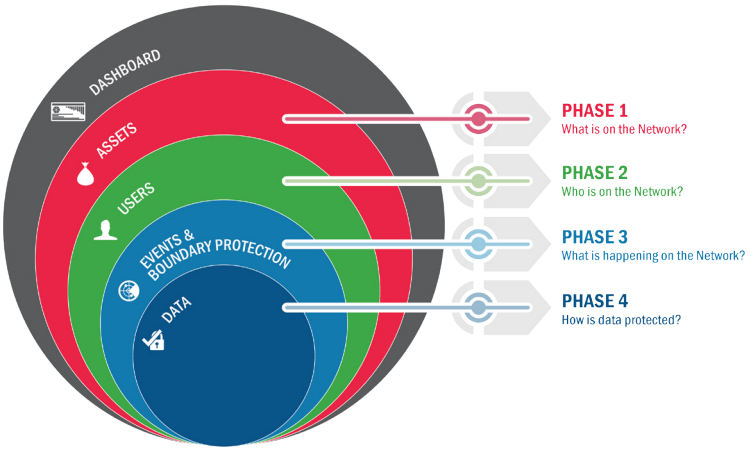
FEDERAL NETWORK PROTECTION

BOTTOM LINE...UP FRONT

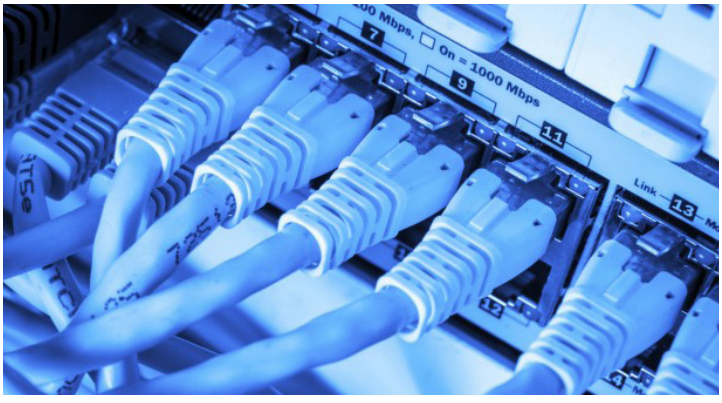
The National Protection and Programs Directorate supports federal departments, agencies and individual stakeholders to secure critical systems from cyberthreats.

WHAT WE DO

- Cyberattacks on Federal Government networks have increasingly become more sophisticated, aggressive and dynamic than in the past, making federal network defense more vital than ever. The Office of Personnel Management's 2014 network intrusion and data theft is just one example of why the U.S. must increase its cyber defenses.
- NPPD exercises its authority under the Federal Information Security Modernization Act of 2014 (FISMA) to administer the information security oversight responsibility of the Office of Management and Budget. NPPD ensures that agencies implement cybersecurity best practices to properly manage risks and also helps in the development of targeted, tactical actions to increase overall cybersecurity.
- NPPD also develops and oversees the development of Binding Operational Directives, coordinates government-wide efforts on information security policies and practices, and provides operational and technical assistance to agencies.
- **Continuous Diagnostics & Mitigation (CDM)** program consists of four phases that form a suite of cybersecurity hardware, software and services whose chief goal is providing each agency situational awareness about their networks. Through the use and application of CDM automated tools and dashboards, agencies can more readily and accurately identify, prioritize and reduce cyber risks.



- The cornerstone of the **National Cybersecurity Protection System (NCPS)** is an intrusion detection and prevention system called EINSTEIN. EINSTEIN 1 provides awareness of intrusion threats; EINSTEIN 2 provides near-real time intrusion detection; and EINSTEIN 3 Accelerated provides real-time prevention of malicious cyber activity.



Homeland Security

ACCOMPLISHMENTS FY 2017

- In addition to supporting the implementation of the Federal Information Security Modernization Act, DHS also helps transform cybersecurity capabilities by:
  - » Providing civilian federal departments and agencies with designs for information security functions;
  - » Identifying common cybersecurity requirements across agencies; and
  - » Deploying cybersecurity specialists to assist small and micro-agencies with government-wide cybersecurity policies and directives.
- 24 CyberStat Program Assessments were conducted for federal department and agencies to improve their information security posture.
- By September 30, 2017, 95 percent of the federal civilian dot-gov user population was covered by EINSTEIN 3 Accelerated, which is an increase of over 55 percent since December 2015.
- Over 500,000 alerts were produced by EINSTEIN using custom signatures and led to 757 reports of possible intrusion attempts to agency partners.
- All agencies falling under the Chief Financial Officer (CFO) Act have deployed at least one intrusion prevention countermeasure from EINSTEIN 3 Accelerated (e.g., DNS sinkholing and email filtering).
- CDM has significantly increased automation for federal agencies, strengthened the management of network devices and eliminated the need to manually count devices.
- CDM Phase 1 tools and dashboards are being used by agencies to automate the identification, detection, remediation and reporting of the operating system vulnerabilities used by critical threats.
- Using its statutory authority, DHS issued two Binding Operational Directive seeking to improve the protection of federal civilian Executive Branch agency networks from cyber threats.

MILESTONES

Phase 1 of the Continuous Diagnostics & Mitigation program resulted in the discovery of roughly 75 percent more assets across agencies than originally reported; in some cases, the increase was greater than 200 percent.

- This comprehensive assessment significantly helped agencies determine what was on their network, the key objective of CDM Phase 1.
- If those connections had remained undetected, they would have been a significant, unmonitored vulnerability to those federal civilian agencies.

During the global ransomware threats, EINSTEIN, CDM, and Automated Indicator Sharing (AIS) played significant roles in protecting federal civilian agencies from worrying.

- EINSTEIN alerts provided enriched information about threats, which enabled agencies to institute measures to better defend their networks.
- With CDM, agencies were able to identify vulnerabilities and flaws in their systems. This helped them determine, prioritize and implement the most appropriate fixes and mitigate vulnerabilities to the WannaCry ransomware attack.
- Automated Indicator Sharing quickly shared machine-readable cyberthreat indicators with nearly 210 participants, and more than 145 were non-federal entities.