NPPD AT A GLANCE

PROACTIVE CYBER PROTECTION

BOTTOM LINE...UP FRONT

The National Protection and Programs Directorate's National Cybersecurity and Communications Integration Center provides 24x7 cyber situational awareness, incident response, a management center, and evaluates the potential consequences of disruptions from physical or cyberthreats and incidents.

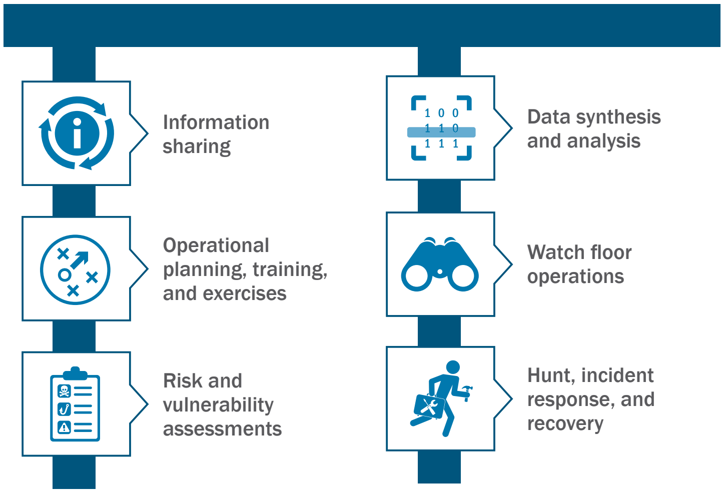
WHAT WE DO

NPPD is responsible for protecting the Nation's critical infrastructure from physical and cyberthreats. This vital mission requires effective coordination and collaboration among a broad spectrum of government and private sector organizations. As part of that collaboration, NPPD provides consolidated all-hazards risk analysis for U.S. critical infrastructure to federal, state and private sector stakeholders.

- The **National Cybersecurity and Communications Integration Center (NCCIC)** focuses on the cyber elements of business, control and communications systems. It maintains and shares cyberthreat information, performs collaborative analysis and conducts incident response to provide timely support. It also ensures that the intersections between cyber and communications are secure and evaluates their impacts on critical physical infrastructure.

Core Functions & Programs

NCCIC performs a suite of functions that provide customers with comprehensive risk management capabilities, products, and services. These functions include:



Information sharing

Operational planning, training, and exercises

Risk and vulnerability assessments

Data synthesis and analysis

Watch floor operations

Hunt, incident response, and recovery

- **Enhanced Cybersecurity Services (ECS)** uses sensitive and classified intrusion detection and prevention capabilities to help protect state, local and U.S.-based private sector computer systems. Please visit *www.dhs.gov/ecs* for enrollment information.

- The **Cyber Information Sharing and Collaboration Program (CISCP)** shares information on cyberthreats, incidents and vulnerabilities with its more than 190 members in near real-time; it also analyzes cyber threats to better understand and improve critical infrastructure network defense.

Homeland Security

- The **Automated Indicator Sharing (AIS)** initiative is part of the NCCIC's effort to create an ecosystem where cyber indicators are shared by companies or federal agencies as soon as they observe an attempted attack. It protects others from a particular threat by making it so that an attack can only be used once. This increases the costs for attackers and, ultimately, reduces the prevalence of cyberattacks. Sharing is also encouraged by congressional legislation which grants liability protection and other protections to companies that participate in AIS.
- The **National Cyber Incident Response Plan (NCIRP)** provides the framework for handling significant cyber incidents. It identifies DHS as the lead for asset response activities and describes how the private sector, states, and federal agencies work together for an integrated national response.

ACCOMPLISHMENTS FY 2017

- AIS shared 3,248 cyber threat indicators with private sector customers.
- 105,972 incidents were reported to NCCIC by government, critical infrastructure and international partners.
- Reduced the median amount of time that federal agencies took to patch critical vulnerabilities from 20 days in 2015 down to 9 days in 2017.
- 58 cyber exercises were completed to test operational readiness and support preparedness among all stakeholders.

MILESTONES

NPPD's key products included assessments of the impacts of cyber and infrastructure disruption in the following cases:

- Assessments of the increase in ransomware threats that may affect healthcare and public health services;
- National risk estimate of Darknet (hidden services on the internet) and its effect on law enforcement and the malware economy; and
- Risks and outcomes of smart grid technologies, plus how they affect the cybersecurity of the Nation's electrical grid.

During the global ransomware attacks in 2017, NPPD collaborated domestically and internationally to protect critical infrastructure and federal networks.

- Conducted malware analysis on multiple samples of the suspected threat vector.
- Collaborated with commercial service providers to discover and share indicators related to the ransomware.
- Helped accelerate threat analysis and information sharing with federal agencies and the private sector.
- Ultimately, very few U.S. entities were affected, and the ransomware attack did not infect federal networks.

The Election Infrastructure Subsector was formally established within DHS in January 2017.

- DHS is actively engaged with state and local officials, as well as relevant private sector entities, to assess the scale and scope of malicious cyber activity potentially targeting U.S. elections.
- NPPD has worked closely with state and local election officials and chartered the Election Infrastructure Subsector Government Coordinating Council in October 2017 to increase information sharing between state, local, non-profit and federal partners to improve the security of the election infrastructure.