NPPD OFFICES

FEDERAL PROTECTIVE SERVICE (FPS)

FPS is responsible for ensuring that the federal workforce and workplace are safe, secure, and resilient across the homeland against acts of violence and other hazards.

OFFICE OF BIOMETRIC IDENTITY MANAGEMENT (OBIM)

OBIM is the DHS enterprise-wide provider of biometric identity services. It provides accurate and timely biometric identity information while also protecting the privacy and civil liberties of individuals.

OFFICE OF CYBER AND INFRASTRUCTURE ANALYSIS (OCIA)

OCIA assists federal, state and local partners in understanding the all-hazards consequences to the Nation's critical infrastructure through integrated analysis, infrastructure prioritization, modeling and simulation.

OFFICE OF CYBERSECURITY AND COMMUNICATIONS (CS&C)

CS&C enables timely response and recovery by coordinating national cybersecurity and emergency communication. It also handles preparedness planning and provisioning for the Federal Government, critical infrastructure owners and operators, as well as other stakeholders.

OFFICE OF INFRASTRUCTURE PROTECTION (IP)

IP leads the coordinated national effort to reduce the risks to our critical infrastructure and help respond and quickly recover after terrorist attacks, natural disasters or other emergencies.

Homeland Security

02132018

NPPD AT A GLANCE

WHO WE ARE

The National Protection and Programs Directorate works with public sector, private sector and government partners to share information, build greater trust, and lead the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

WHAT WE DO

America is a nation of communities and neighborhoods, of relationships, values and laws. We are also a nation of networks and systems that we rely on for just about everything we do—from communicating and traveling to banking and shopping.

The critical infrastructure that supports all of this and enables our way of life is vulnerable. It is vulnerable to an ever-evolving array of threats, ranging from extremist and cyberattacks to natural disasters like hurricanes or floods.

Reducing the risks from these threats and making our physical and digital infrastructure more resilient and secure is NPPD's abiding mission.

NPPD is continually working proactively with partners to make sure that the systems and networks that Americans rely on are there when they need them. NPPD strives to protect the physical and cyber infrastructure that we rely on and make it more resilient to what we cannot prevent.

LEARN MORE ABOUT NPPD!

For additional information, please visit *www.dhs.gov/nppd.*

- FEDERAL NETWORK PROTECTION
- PROACTIVE CYBER PROTECTION
- INFRASTRUCTURE RESILIENCE & FIELD OPERATIONS
- BIOMETRIC IDENTITY MANAGEMENT
- FEDERAL FACILITY PROTECTION

Homeland Security

OVERVIEW

2007 ESTABLISHED

3,477 EMPLOYEES

9,000 FEDERAL FACILITIES PROTECTED

2,000 FACILITY SECURITY ASSESSMENTS

106,000 CYBER INCIDENT REPORTS

90,000 TRAINED ONLINE IN ACTIVE SHOOTER PREPAREDNESS

95% FEDERAL CIVILIAN WORKFORCE COVERED BY ADVANCED CYBER PROTECTION

100% NATIONAL SPECIAL SECURITY EVENTS SUPPORTED IN 2017

100 Million BIOMETRIC IDENTITY TRANSACTIONS

SNAPSHOT OF OUR WORK

NPPD partners with government and the private sector to protect and secure the people, places, spaces, data and networks that make America run. NPPD's daily efforts make the Nation's cyber and physical infrastructure more secure and resilient.

Every day, NPPD employees:

- Share information with critical infrastructure partners and stakeholder and serve as the national hub for cybersecurity and communications **information data sharing** in near-real-time.
- Conduct **federal network protection** for federal departments, agencies and individual stakeholders to secure critical systems from cyber threats.
- Serve as **cyber and physical security experts** in advancing security operational capabilities by developing processes, tools, and technologies to assess threats and vulnerabilities.
- Provide **capacity-building** technical assistance, tools, exercises, and training programs that focus on enhancing awareness and understanding of common risks and possible mitigation strategies for the critical infrastructure community.
- Serve as the lead for coordinating asset response activities with the private sector, states, and federal agencies for an integrated **incident response** to cyber incidents, and assess and inform risk management strategies on the consequences of emerging and future risks.
- Develop and enhance capabilities to support crisis action by identifying and prioritizing infrastructure through the use of **analysis and modeling** capabilities.
- Work to proactively take on greater identity services responsibilities and set the framework for a continuous evolution within DHS to create robust **biometrically based identity services** while protecting privacy and civil rights and civil liberties.
- Strengthen and build capabilities that enhance **Federal facility protection** operations to reduce the impact of criminal incidents or terrorist activities in, around, or to Federal facilities, their employees, and visitors.
- Manage the **regulatory compliance** of securing chemical facilities through the Chemical Facility Anti-Terrorism Standards program.

PERFORMANCE HIGHLIGHTS, FY 2017

- Conducted more than **200 classified and unclassified meetings** with critical infrastructure partners to share actionable information and recommend preventative measures.
- Received nearly **106,000 cyber incident reports** from federal and critical infrastructure partners. Conducted 23 on-site responses to cyber incidents and identified over 129,000 cybersecurity vulnerabilities through scans and vulnerability assessments.
- **Deployed EINSTEIN 3 Accelerated (E3A)** capabilities that have the **capacity to protect 500,000 federal users from malicious e-mail attacks** (e.g., e-mail-initiated spearphishing campaigns) or malware installed on dot-gov networks.
- **Supported infrastructure and supply chain restoration** in states and territories hit by hurricanes Harvey, Irma, and Maria.
- **Established the Election Task Force** and hosted the first Government Coordinating Council to create information sharing protocols and enable state and local officials to share classified threat information.
- Conducted **2,270 Hometown Security Initiative activities** in FY 2017, supporting the needs of small and mid-sized business and local communities.
- Conducted **60 active shooter preparedness workshops in FY 2017 across the country with 6,000 participants.** More than 90,000 people have done the active shooter training on-line.
- Through the **Office for Bombing Prevention, conducted 211 in-person workshops** in 36 states, Washington, D.C., and Canada with 5,138 stakeholders, including law enforcement and other emergency services personnel, critical infrastructure owners and operators, and security staff. Also provided 405 virtual instructor-led trainings to 5,327 partners.
- Under the Chemical Facility Anti-Terrorism Standards program, NPPD has **successfully approved more than 2,700 Site Security Plans or Alternative Security Programs** for high-risk chemical facilities. It has also conducted more than 3,000 authorization inspections and 3,000 compliance inspections to date.
- In response to a series of high profile attacks targeting government facilities and officials overseas, **NPPD surged the presence of law enforcement and security experts at Federal Government buildings** in several cities. This improved the immediate security of 189 facilities and over 87,000 tenants.
- Processed more than **100 million biometric transactions,** resulting in more than 1.1 million derogatory matches that aided the decision-making of mission partners.
- Completed over **184 technical assistance engagements on communications operability and interoperability in 47 states and territories.** These included 16 statewide comprehensive communication planning workshops and 12 interoperable communications capabilities analyses of public safety communications in conjunction with major city police departments and public safety disciplines at all levels of government.
- **Produced 132 analytic products during the 2017 hurricane season** which were accessed more than 400,000 times by key partners.