NPPD AT A GLANCE

National Protection and Programs Directorate
Leading the national effort to strengthen the security and resilience of the nation's physical and cyber infrastructure

WHO WE ARE & WHAT WE DO

America has always been a nation of communities and neighborhoods, of relationships, values, and laws. Today, we're also a nation of networks and systems, ones we rely on for just about everything we do — from communicating and traveling to banking and shopping.

But the infrastructure that supports all of this — that enables our way of life — is vulnerable. It's vulnerable to an ever-evolving range of threats, from terrorist or cyber attacks to natural disasters, like hurricanes or floods.

That's where NPPD comes in. Why? Because reducing the risks from these threats, and making our physical and digital infrastructure more resilient and secure, is our abiding mission. Every day, the men and women of NPPD work across DHS, and around the country, to strengthen the very backbone of our national and economic security.

Often, we're behind the scenes, making sure that the systems and networks Americans rely on are there when we need them.

In the homeland security world, as DHS Secretary Johnson has said, "No news is good news." For NPPD, no news is the result of hard work, vigilance, and dedication by people working to prevent bad things you never hear about, or help the public prepare itself and recover from the storm we cannot prevent.

National Cybersecurity and Communications Integration Center (NCCIC)

LEADERSHIP

DHS Secretary:	Jeh Johnson
DHS Deputy Secretary:	Alejandro Mayorkas
Under Secretary, National Protection & Programs Directorate:	Suzanne Spaulding
Deputy Under Secretary, Cybersecurity & Communications:	Dr. Phyllis Schneck
Deputy Under Secretary (acting):	David Hess
Chief of Staff, NPPD (acting):	Steven Harris
Assistant Secretary, Cybersecurity & Communications:	Dr. Andy Ozment
Assistant Secretary, Infrastructure Protection:	Caitlin Durkovich
Director, Federal Protective Service:	L. Eric Patterson
Director, Office of Biometric Identity Management (acting):	Shonnie Lyon
Director, Office of Cyber and Infrastructure Analysis:	John Murphy

SNAPSHOT OF OUR WORK

NPPD works with partners at all levels of government, and from the private and non-profit sectors, to share information and build greater trust to make our cyber and physical infrastructure more secure.

On a typical day, NPPD employees:

- Issue dozens of actionable cybersecurity alerts to the private sector and general public to help protect against threats.
- Work with State and local officials to plan security for large public gatherings, such as Times Square New Year's Eve, the Presidential Inauguration, and the Super Bowl.
- Meet with dozens of owners and operators — from chemical plants and electric utilities to shopping malls — to help them assess and mitigate potential risks from terrorist attacks and natural disasters.
- Protect more than 9,500 Federal facilities and screen thousands of daily visitors, while keeping out hundreds of prohibited items.
- Process roughly 2,000 identity verifications in a timely and secure manner while protecting individuals' privacy, civil rights, and civil liberties.

OVERVIEW

Established: 2007
Employees: 3,000
Field Offices: 230 cities
Protective Security Advisors: 90
Chemical Facility Inspectors: 130
Federal Law Enforcement Officers: 900
Total Field Personnel: 1,500

"Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure – including assets, networks, and systems – that are vital to public confidence and the Nation's safety, prosperity, and well-being." **Presidential Policy Directive 21 — Feb. 12, 2013**

KEY NPPD OFFICES

Federal Protective Service (FPS) is a Federal law enforcement agency that provides integrated security and law enforcement services to federally owned and leased buildings and facilities.

Office of Biometric Identity Management (OBIM) supports DHS missions with accurate, timely biometric identity information, while protecting the privacy and civil liberties of individuals.

Office of Cyber and Infrastructure Analysis (OCIA) provides integrated, all-hazards consequence analysis to illuminate the interdependence of our Nation's cyber and physical critical infrastructure.

Office of Cybersecurity and Communications (CS&C) has the mission of assuring the security, resiliency, and reliability of the Nation's cyber and communications infrastructure.

Office of Infrastructure Protection (IP) leads the coordinated National effort to reduce risk to our critical infrastructure and help respond and quickly recover in case of terrorist attacks, natural disasters, or other emergencies.

Office of the Under Secretary (OUS) works with liaisons across NPPD and provides Directorate leadership, oversight, and support for our more than 3,000 employees nationwide.

LEARN MORE & PARTNER WITH US

See how your organization or business can work with NPPD to help make all of us more secure:

dhs.gov/cyber
dhs.gov/critical-infrastructure

C3 VOLUNTARY PROGRAM

STOP | THINK CONNECT

PERFORMANCE HIGHLIGHTS FY2013

- Brought our two major watch operations — the National Infrastructure Coordinating Center (NICC) and the National Cybersecurity and Communications Integration Center (NCCIC) — together in a single location to integrate our analysis and awareness of threats to both our nation's cyber and physical infrastructure.
- Increased active shooter preparedness via a training program for more than 3,300 Federal facility tenants and through a new online training portal that combines knowledge from across DHS, and that reached more than 2,400 real-time participants in an active shooter virtual round table.
- Worked with thousands of leaders from the critical infrastructure community at more than 300 engagements to implement the President's Executive Order and Presidential Policy Directive to strengthen our nation's cybersecurity, resilience, and critical infrastructure.
- Trained more than 11,000 State, local, and private law enforcement partners on awareness and response strategies around potential Improvised Explosive Devices (IEDs).
- Completed almost 700,000 identity verifications and 4.6 million latent print comparisons, resulting in more than 1,200 identifications, while maintaining a standard response time of 10 minutes or less for 92% of all urgent verification requests.
- Worked with States and multiple Water & Wastewater Sector facilities to offer site-specific options to mitigate potential physical consequences from exploited cyber vulnerabilities.
- Helped the public stay safe through National Cyber Security Awareness Month, Critical Infrastructure Security and Resilience Month, the Stop. Think. Connect.™ campaign, the "If You See Something, Say Something"™ campaign, and hundreds of partner events.

FPS Securing a Federal Facility

"DHS must continue efforts to address the growing cyber threat, illustrated by the real, pervasive, and ongoing series of attacks on things like stores, banks, email services, power substations, and the public that depends on them." **DHS Secretary Jeh Johnson — Feb. 7, 2014**