



U.S. Department of Homeland Security Protective Security Advisor (PSA) North Carolina District



“Securing the Nation’s critical infrastructures one community at a time”



Critical Infrastructure & Key Resources (CIKR)

- What is CIKR?
 - Assets, systems, and networks, whether physical or virtual, so vital to the United States that the incapacity or destruction would have a debilitating impact on national and economic security, public health and safety, or any combination of these matters



The Threat

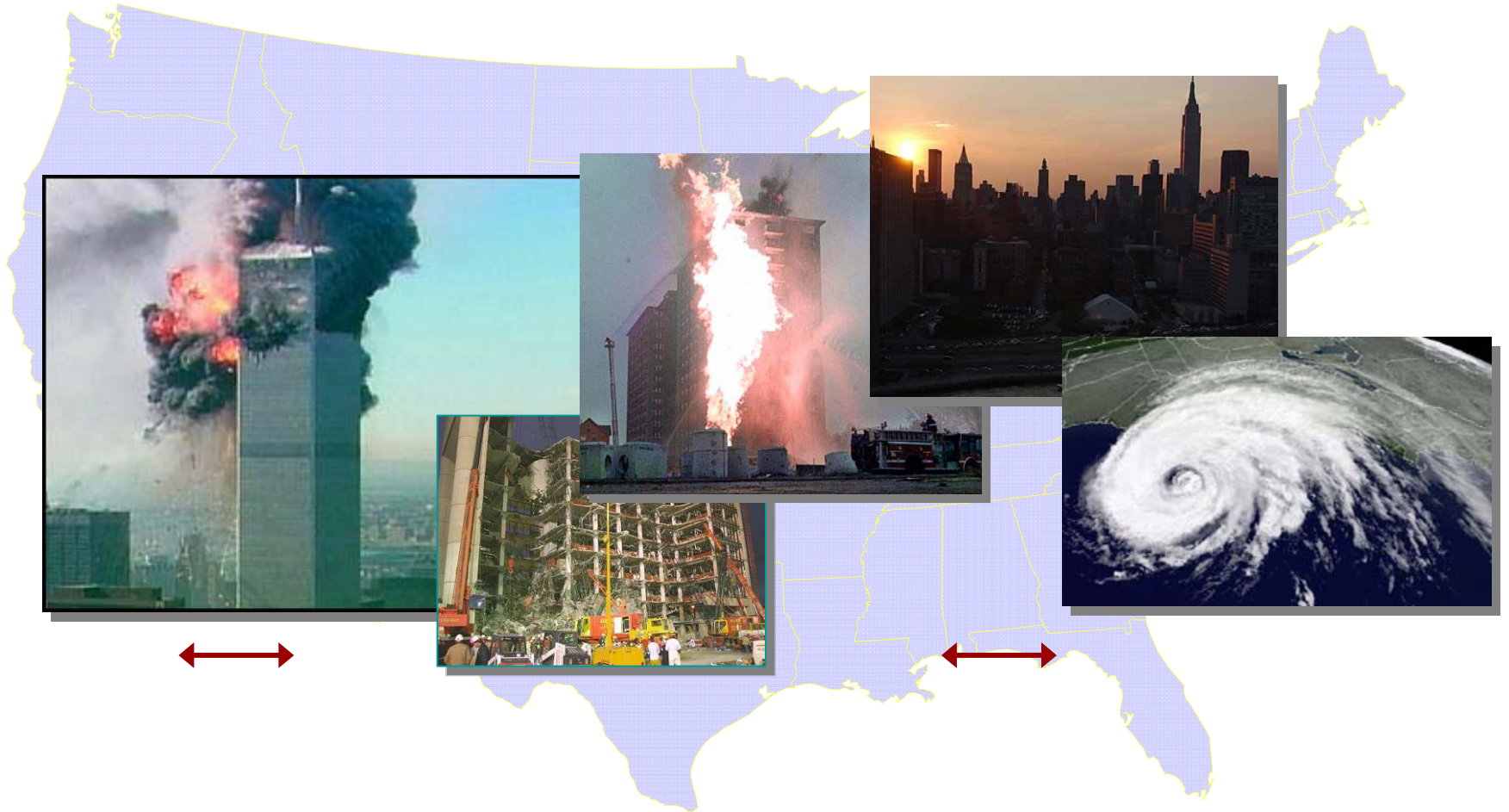


We will “hit hard the American economy at its heart and its core.”

- Osama bin Laden

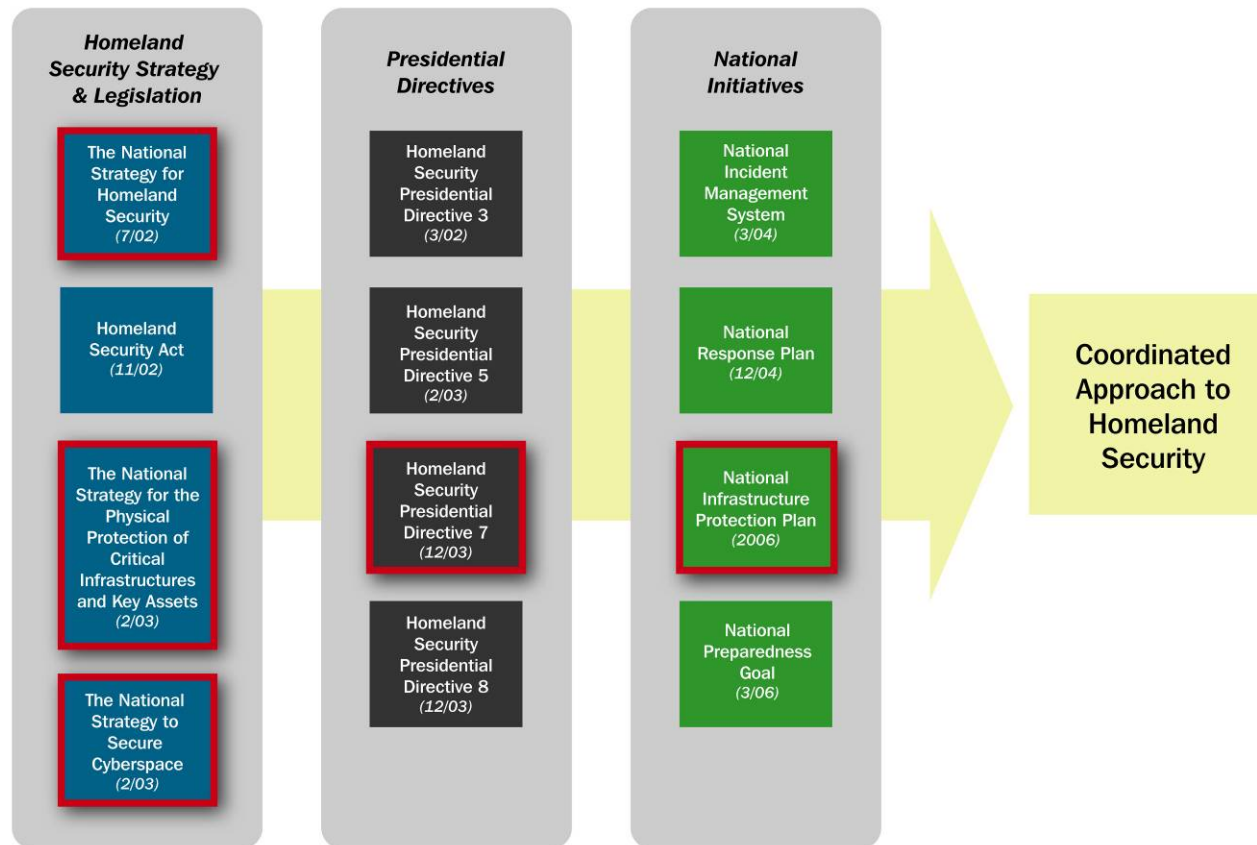


Threats May Come From All Hazards



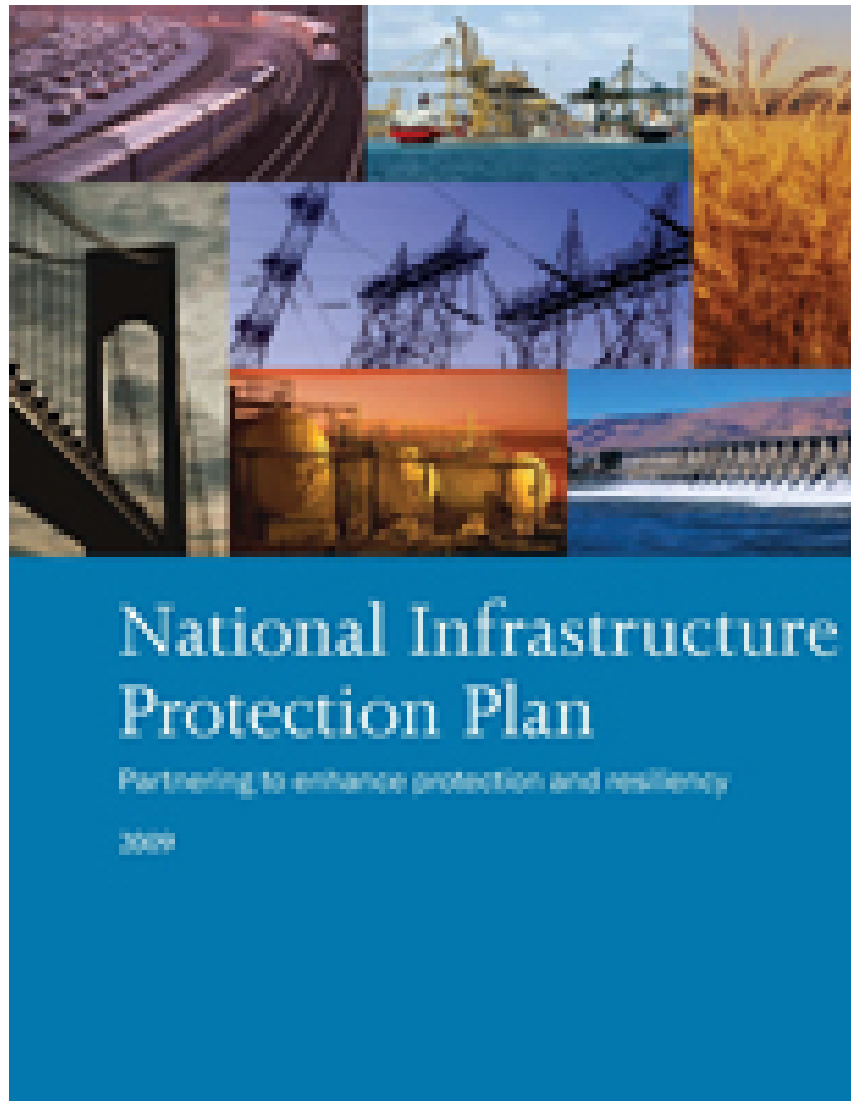


Homeland Security Strategic Framework





National Infrastructure Protection Plan





NIPP Goal

Build a safer, more secure, and more resilient America by enhancing protection of the Nation's CIKR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.





The Role of the Homeland Security National Infrastructure Protection Plan (NIPP)

- Unify a national effort to secure America
- Prevent and deter terrorist attacks
- Protect against and respond to threats and hazards to the nation
- Respond to and recover from acts of terrorism, natural disasters, or other emergencies
- Coordinate the protection of our nation's critical infrastructure across all sectors



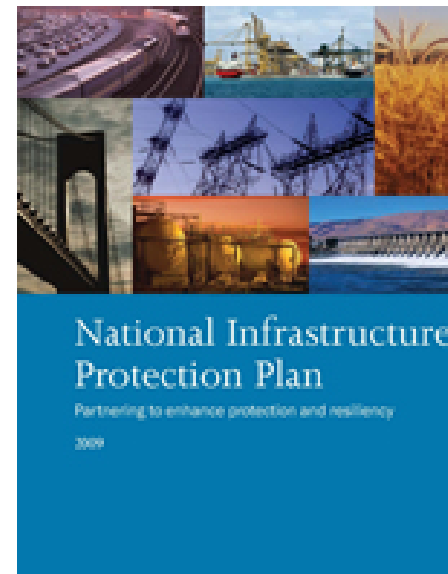
18 Critical Infrastructure & Key Resource Sectors

Critical Infrastructure Sectors

- Agriculture and food
- Banking and finance
- Chemical
- Critical Manufacturing
- Defense industrial base
- Emergency services
- Energy
- Information technology
- Postal and shipping
- Public health and healthcare
- Telecommunications
- Transportation systems
- National monuments and Icons
- Drinking water and water treatment systems

Key Resources

- Commercial facilities
- Dams
- Government facilities
- Nuclear reactors, materials, and waste





Agriculture and Food

Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan

May 2007

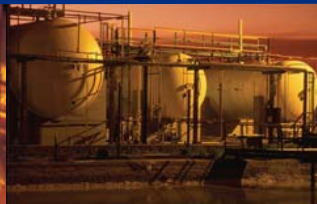
*Combines both the U.S. Department of Agriculture and the U.S. Department of Health and Human Services' Food and Drug Administration portions of the plan.



Banking and Finance

Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan

May 2007



Chemical

Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan

May 2007



Defense Industrial Base

Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan

May 2007



Energy

Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan

May 2007



Emergency Services

Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan

May 2007



Information Technology

Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan

May 2007



Communications

Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan

May 2007



Postal and Shipping

Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan

May 2007



Public Health & Healthcare

Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan

May 2007



Transportation Systems

Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan

May 2007



Water

Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan

May 2007



National Monuments & Icons

Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan

May 2007



Commercial Facilities

Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan

May 2007



Government Facilities

Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan

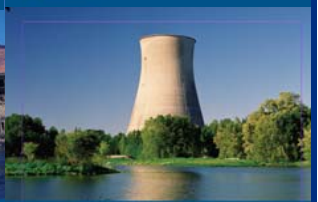
May 2007



Dams

Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan

May 2007



Nuclear Reactors, Materials, and Waste Sector

Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan

May 2007





National Monuments & Icons

Critical Infrastructure and Key Resources
Sector-Specific Plan as input to the
National Infrastructure Protection Plan

May 2007



Department of
**Homeland
Security**



Department
of the Interior

Homeland
Security



TAXONOMY NATIONAL MONUMENTS AND ICONS

- **13. NATIONAL MONUMENTS AND ICONS**
- 13.1 NATIONAL MONUMENT/ICON STRUCTURES
 - 13.1.1 Buildings
 - 13.1.2 Monuments and Memorials
 - 13.1.3 Other Monument/Icon Structures
- **13.2 NATIONAL MONUMENT/ICON GEOGRAPHIC AREAS**
- 13.2.1 Parks and Public Lands
- 13.2.2 Historical and Heritage Lands
- 13.2.3 Other Monument/Icon Geographic Areas
- **13.3 NATIONAL MONUMENT/ICON DOCUMENTS AND OBJECTS**
- 13.3.1 Historical/Significant Documents
- 13.3.2 Historical/Significant Objects
- **13.4 OTHER NATIONAL MONUMENTS AND ICONS**



Data Call Criteria National Monuments and Icons Sector

- For the FY2009 data call, states and territories are not being asked to propose national monuments and iconic assets.
- The Tier list for the National Monuments and Icons sector will be based on an established critical asset identification methodology utilized by the Sector Specific Agency (the Department of Interior).
- This methodology identifies sector assets of unique quality and that are widely recognized both nationally and internationally to be symbolic of the United States.



Identify Assets

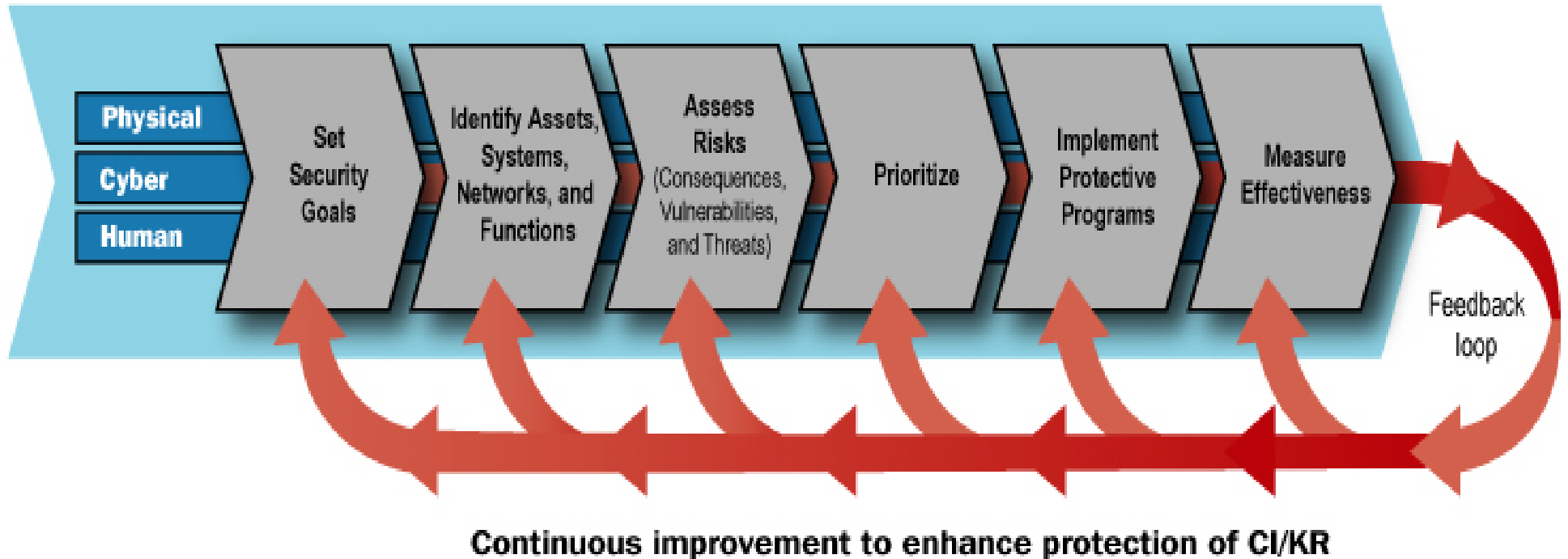
- What is out there?
- What is important?
- What are the consequences?
- What are the vulnerabilities?
 - Physical
 - Cyber
 - Human





NIPP Risk Management Framework

The NIPP and supporting Sector-Specific Plans (SSPs) describe the processes to:





How do we think about risk?

CONSEQUENCE (C)

(Criticality) – Estimate of what could happen to people, the economy, national psyche, or mission capability

VULNERABILITY (V)

Estimate of how easy or difficult it would be to successfully attack the asset and, in so doing, yield the most severe consequence

THREAT (T)

Application of threat to the asset, in terms of enemy Capability and Intent, well-informed by both C and V values

RISK

**Comparative across all infrastructure
– Allows the creation of a risk-based list of Critical National Infrastructure
– Supports the allocation of Federal Assets**



The Challenge to Protect Critical Infrastructures & Key Resources (CIKR)

- 85% of all critical infrastructures and key resources are privately-owned
- Homeland Security must work together with industry and state, territorial, local, and tribal governments to protect critical infrastructures and key resources
- Protective Security Advisors (PSA) placed around the country to help communities better protect the Nation's assets



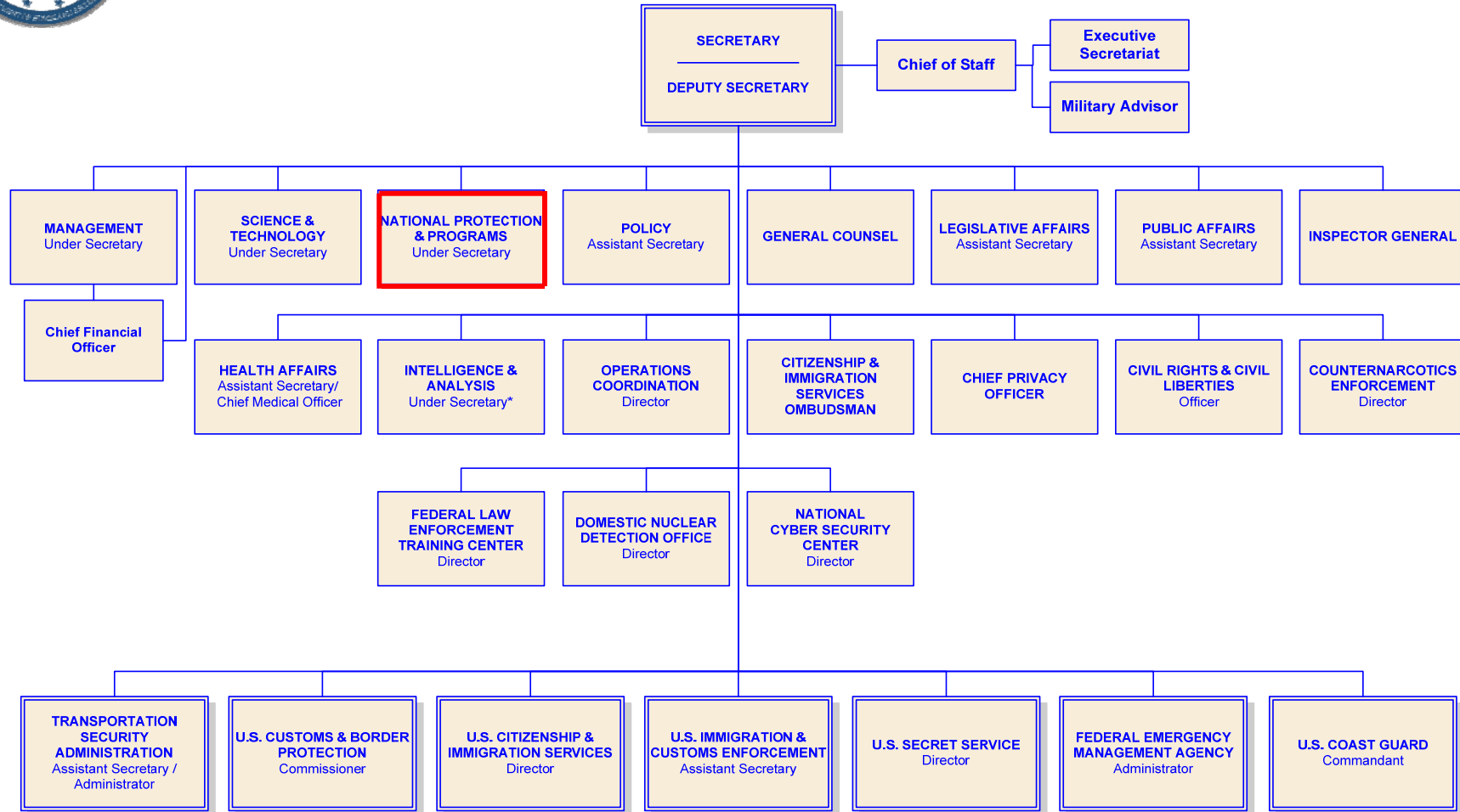
The Department of Homeland Security Provides Community-Based Support

Protective Security Advisors will:

- Assist with ongoing local and state critical infrastructure security efforts which are coordinated by the state Homeland Security Advisors
- Support the development of the national risk picture by identifying, assessing, monitoring, and minimizing risk to critical assets at the local level
- Upon request, facilitate and coordinate vulnerability assessments of local CIKR
- Provide reach-back capability to the Department of Homeland Security and other Federal government resources



U.S. DEPARTMENT OF HOMELAND SECURITY

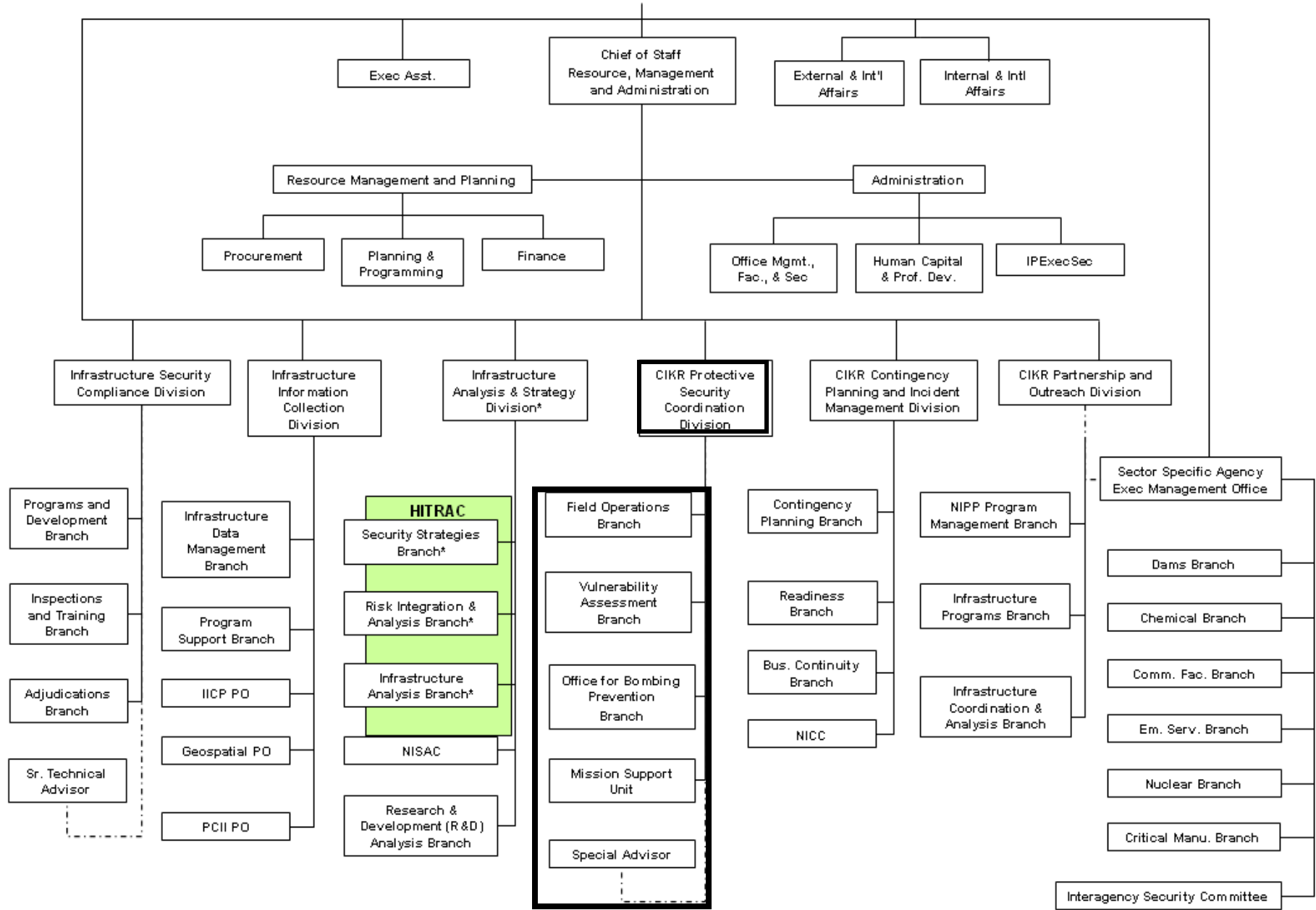


* Under Secretary for Intelligence & Analysis title created by Public Law 110-53, Aug. 3rd, 2007

Approved 3/20/2008

OFFICE OF INFRASTRUCTURE PROTECTION

Office of the Assistant Secretary for Infrastructure Protection





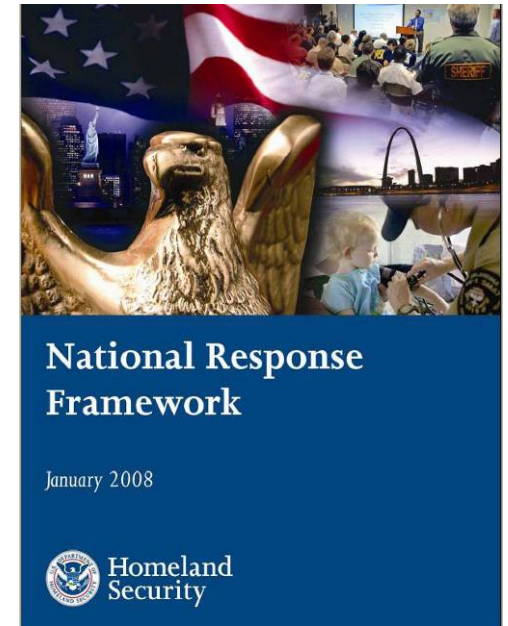
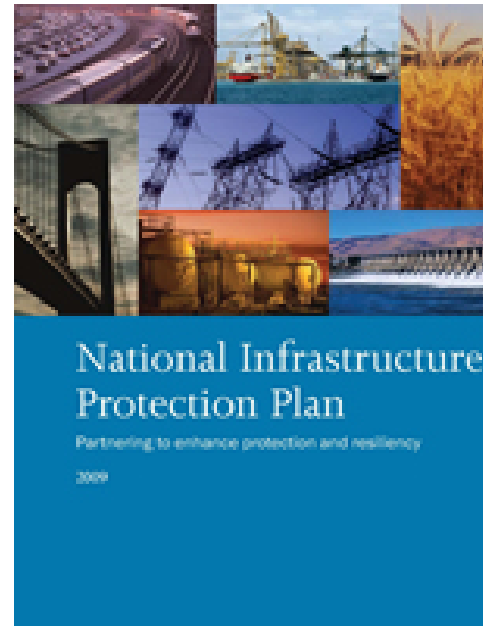
Protecting Critical Infrastructure and Key Resources

National Infrastructure Protection Plan

- Working together with State, local, territorial, tribal governments and the private sector to protect critical infrastructures and key resources

National Response Framework

- Providing situational awareness and technical assistance in accordance with the National Response Framework and CIKR Support Annex as necessary



CIKR Support Annex

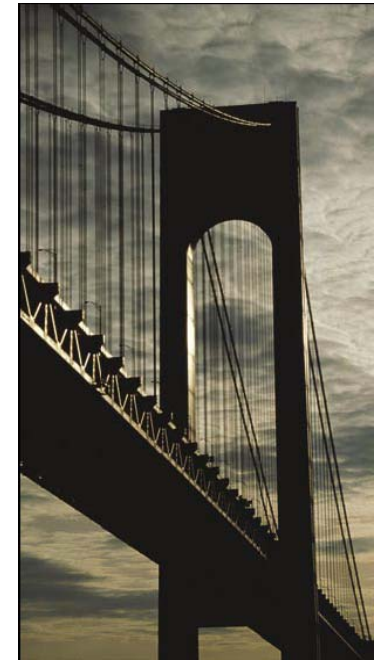


Homeland
Security



Enhanced Critical Infrastructure Protection (ECIP) Visit

- Led by the Office of Infrastructure Protection (IP).
- Initial and follow-up visits of state's high-priority critical infrastructure key resources.
- Accomplished by regional Protective Security Advisors (PSA).
- Coordinated with Homeland Security Advisor (HSA), Sector Specific Agencies (SSA), the Federal Bureau of Investigation (FBI), and Federal, State, territorial, local, tribal and private sector representatives.





Enhanced Critical Infrastructure Protection Resources

- Homeland Security Information Network
- Protected Critical Infrastructure Information
- Private Sector Clearance Procedures
- Vulnerability Assessments
- Surveillance Detection and Soft Target Awareness Courses
- Technical Resource for Incident Prevention
- Automated Critical Asset Management System



Vulnerability Assessments and Surveys

Overview

- The Buffer Zone Protection Program (BZPP)
- Regional Resiliency Assessment Program (RRAP)
- Site Assistance Visits (SAVs)
- Comprehensive Review (CR)
- Infrastructure Survey Tool (IST)



Surveillance Detection and Soft Target Awareness Courses


- Soft Target Awareness Course (STAC) - facility managers, supervisors and security staff
- Surveillance Detection Training for Commercial Infrastructure Operators and Security Staff Course (SD CIKR) - facility managers, supervisors and security staff (Nationally Significant Infrastructure)
- Surveillance Detection Training for Municipal Officials, State and Local Law Enforcement Course (SD LLE)



TRIPwire

Technical Resource for Incident Prevention





TRIPwire

Technical Resource for Incident Prevention


HOME ABOUT GLOSSARY MY ACCOUNT CONTACT US LOGOUT

FOR OFFICIAL USE ONLY

WELCOME

TRIPwire is a dynamically-integrated network sponsored by the Department of Homeland Security's Office for Bombing Prevention (DHS/OBP). TRIPwire provides its users with information regarding terrorist tactics, techniques, and procedures relevant to improvised explosive device (IED) use.

View the TRIPwire demo.



MEMBER DIRECTORY

State:

Current Assignment:

ATF Squad
Bomb Squad
Counterterrorism Unit
DHS Office for Bombing Prevention

Advanced Search Search Reset

EVENT CALENDAR

Critical Infrastructure Protection Training Program (CIPTP)
Glynn, GA
05/21/2007

SpecOps West 2007 Symposium & Expo
Tacoma, Washington
06/04/2007

IED 2007 Symposium & Expo
Fayetteville, North Carolina
05/11/2007

View All Events

Admin Links

Get Excel Data
Locked User utility

WHAT'S NEW

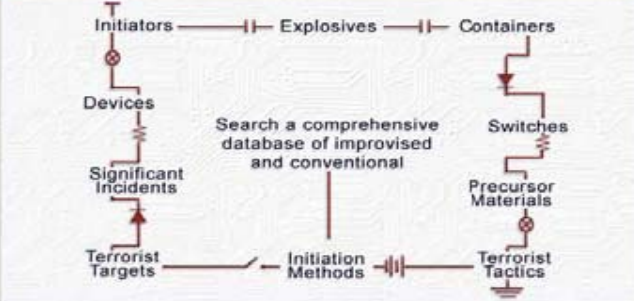
CURRENT THREAT LEVEL **ELEVATED**

BREAKING NEWS: Chlorine bomb hits Iraq village
A bomb detonated in the Diyala province of Iraq killing 32 people and 50 injured in a suspected chlorine bomb attack. Reports claim that the nature of the victims' burns suggests poison gas. This attack could imply tactical developments following last month's chlorine bomb that killed 35 people in Ramadi.

Suicide bombing at hotel in Pakistan city near Afghan border kills 25
A suicide attacker detonated a bomb that ripped through the Marhaba hotel restaurant in Peshawar, Pakistan, near the Afghan border, killing at least 27 people. Authorities report that the bomber was targeting American spies. Severed legs found on the scene indicate a waist-worn device as opposed to a suicide vest where there is usually the discovery of a decapitated head.


*Need Help?

TRIPwire DIRECTORY



Search a comprehensive database of improvised and conventional

TRITON REPORTS




Quick Look Report - Suicide IED Attack on Marhaba Hotel Peshawar Pakistan, 15 May 2007
TRITON Quick Look Report
2007-05-15

Quick Look Report - Suicide IED Attack on Pakistani Interior Minister, Charsadda, 28 April 2007
TRITON Quick Look Report
2007-04-30

EMAIL INBOX

1 Total Messages
View Inbox

COMMUNITY FORUM



Connect with members of the bombing prevention community around the country and discuss a variety of topics.

Enter Forums >

TRIPwire LIBRARY

Government Resources
Terrorist Videos
Threat Alerts
Terrorist Documents
Law Enforcement Awareness
Private Sector Outreach


IN THE NEWS

Car bomb near Shiite market kills 32; new attacks hit Baghdad Green Zone

Car bomb near Shiite market kills 32; new attacks hit Baghdad Green Zone

9 more Madrid terror trial suspects join hunger strike

Suspicious package turns out to be take-out

View All Stories
All stories provided by 



ACAMS...
is fully funded by DHS and is intended to be free to
the public safety sector nationwide

ArchAngel - Windows Internet Explorer

https://michael.lapsc.org/menu.asp

File Edit View Favorites Tools Help

Google G Go Bookmarks 253 blocked Check AutoLink AutoFill Send to Settings

ArchAngel

Automated Critical Asset Management System

White, Stephen

Constellation Log Off

Home Inventory Asset Manager Questionnaire Initial Asset Visit Reports Admin Search Resources

The diagram illustrates the ArchAngel system architecture, divided into two main phases: **Prevention** and **Response**.

Prevention Phase:

- Data Collation:** Receives input from the **POLICE** (Department of Justice) and the **U.S. Department of Homeland Security**.
- Constellation:** A central hub that feeds into the **Inventory** and **AMQ** (Asset Manager Questionnaire).
- Inventory:** Feeds into **AMQ** and **IAV** (Initial Asset Visit).
- AMQ:** Feeds into **IAV**.
- IAV:** Feeds into the **Reports** section.

Response Phase:

- Security:** Feeds into the **ARCHANGEL** core system.
- Mapping:** Feeds into the **ARCHANGEL** core system.
- Resources:** Feeds into the **ARCHANGEL** core system.
- Reports:** Feeds into the **ARCHANGEL** core system.
- Custom Reports:** Feeds into the **ARCHANGEL** core system.
- Pre-Incident:** Feeds into the **ARCHANGEL** core system.
- CARVER:** Feeds into the **ARCHANGEL** core system.
- Data Call:** Feeds into the **ARCHANGEL** core system.

The **ARCHANGEL** core system is highlighted in a red box and is labeled **LAW ENFORCEMENT SENSITIVE**.

Additional components include **BZPP** (Bureau of Zoning and Planning) and **MSHARRPP+V** (Missouri State Highway Patrol and Vehicle).



On Going Initiatives

- Enhanced Critical Infrastructure Protection (ECIP) visits and Infrastructure Survey Tool (IST) collection on Infrastructure sites of National significance
- Enhanced GIS Infrastructure Products
- Statewide Infrastructure Protection Program (SIPP)



DHS Contact Information

Darryl Aspey
Protective Security Advisor
North Carolina District
Raleigh, NC 27609
(919) 855-1042
darryl.aspey@dhs.gov



Homeland Security

Homeland
Security



Information Sharing and Protection



The network approach to information sharing and protection enables secure multidirectional information sharing between security partners.



Protected Critical Infrastructure Information (PCII)

- The Protected Critical Infrastructure Information (PCII) Program
- Established pursuant to the Critical Infrastructure Information Act of 2002 (CII Act)
- Creates a new framework which enables members of the private sector to voluntarily submit sensitive information regarding the Nation's critical infrastructure to the DHS with the assurance that the information, if it satisfies the requirements of the CII Act, will be protected from public disclosure.



National Monuments and Icons Sector

- The economic impact of an attack may significantly affect the local and national tourism industry
- The greatest potential impact will be on the national psyche
- An attack on a National Critical asset could result in significant loss of life and intense media coverage with visual reminders of the death and destruction.
- It could also reduce public confidence in our Nation's ability to protect its citizens and resources against attack.



Dependency on our Critical Infrastructures & Key Resources...

- National Security
- Economic Vitality
- Our Way of Life

Attacks Could...

- Disrupt government and private industry operations and impact our economy and society
- Result in large-scale human casualties, property destruction, and damage to national prestige and public confidence

