

# The Industry Pilot Series™: U.S HOMELAND SECURITY

The Industry Pilot Series™ provides readers with an in-depth overview of key industry sectors. Identifying industries that genuinely interest you is a key, and often overlooked, aspect of effective career planning. Industry Sectors covered thus far include: Financial Services, Healthcare, Homeland Security, and Biotechnology. Excerpts for each are available free at [SilverCareerManagement.com](http://SilverCareerManagement.com).

## ***Contents:***

- Industry Snapshots
- Homeland Security: General Introduction
  - *Definition*
  - *Importance/ Objective*
  - *Implementing the National Strategy for Homeland Security*
  - *Organizing for a secure Homeland*
- Issues Dealt by Homeland Security
  - *Intelligence and Warning*
  - *Border and Transportation Security*
  - *Domestic Counter terrorism*
  - *Protecting Critical Infrastructures and Key Assets*
  - *Defending against Catastrophic Threats*
  - *Emergency Preparedness and Response*
- Foundations
  - *Science & Technology*
  - *Information Sharing and Systems*
  - *International Cooperation*
- Investments/ Budget for Department of Homeland Security
  - *Spending on Homeland Security*
  - *Forecast Spending on Homeland Security*
- Priorities for the future
- Employment Trends
- Federal Homeland Security Agencies and Organizations
- List of Homeland Security Companies

## Industry Snapshots

- Marketplace forecasts for the global homeland security industry anticipate business will grow from approximately \$40 billion in 2004, to nearly \$180 billion by 2015 <sup>1</sup>
- Cybersecurity is expected to be the fastest growing sub-sector of homeland security business from 2005 through 2010, with an annual growth rate of 15% to 20% <sup>2</sup>
- The median annual compensation for security professionals in the United States in 2004 was \$75,200, a 5.9% increase over the 2003 level, outpacing inflation <sup>3</sup>
- The majority of homeland security is performed in the private sector, with 85% of all critical infrastructures privately controlled and 35% of all U.S. companies planning to invest in and expand security programs in 2005 <sup>4</sup>

## Homeland Security: General Introduction

### Definition

Homeland security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, minimize the damage and orchestrate recovery efforts in the event attacks occur.

The term became prominent in the United States following the September 11, 2001 attacks; it had been used only in limited policy circles prior to 9/11. Before this time, such action had been classified as civil defense. Because the US Department of Homeland Security (DHS) includes the Federal Emergency Management Agency (FEMA) it has responsibility for preparedness, response and recovery to natural disasters as well.

### Importance/Objective of Homeland Security

Homeland security involves efforts both at home and abroad. It demands a range of government and private sector capabilities. And it calls for coordinated and focused effort from many actors who are not otherwise required to work together and for whom security is not always a primary mission.

The National Strategy for Homeland Security establishes three objectives based on the definition of homeland security:

- Prevent terrorist attacks within the United States
- Reduce America's vulnerability to terrorism
- Minimize the damage and recover from attacks that do occur

### Implementing the National Strategy for Homeland Security

---

<sup>1</sup> Homeland Security Research Corporation estimate

<sup>2</sup> Frost & Sullivan Analysis of Current and Future U.S. Homeland Security Market

<sup>3</sup> ASIS U.S. Security Salaries Survey Results, 2005

<sup>4</sup> ASIS International Foundation Trends Report, 2005

The National Strategy for Homeland Security aligns and focuses homeland security functions into *six critical mission areas: intelligence and warning, border and transportation security, domestic counterterrorism, protecting critical infrastructure and key assets, defending against catastrophic terrorism, and emergency preparedness and response*. The first three mission areas focus primarily on preventing terrorist attacks; the next two on reducing our Nation’s vulnerabilities; and the final one on minimizing the damage and recovering from attacks that do occur.

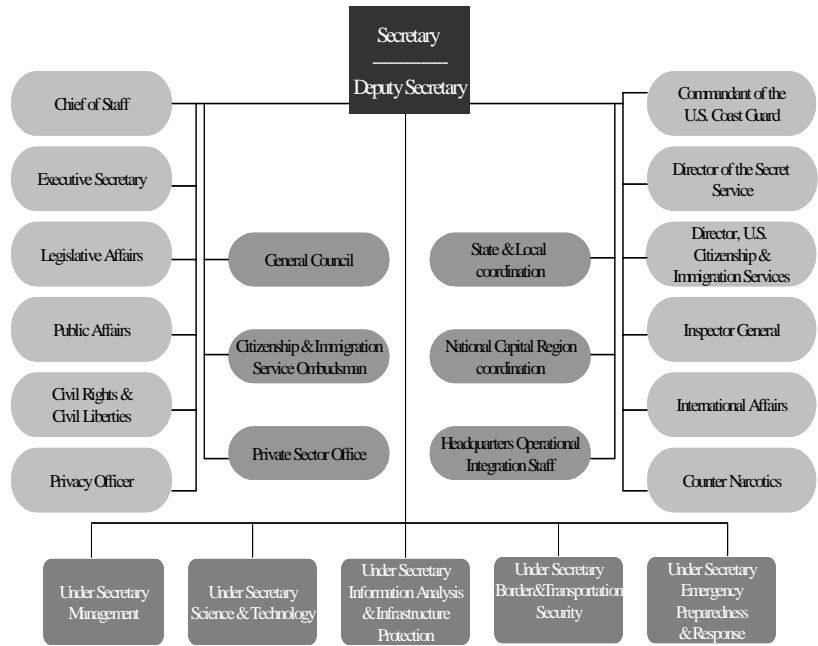
It provides a framework to align the resources of the federal budget directly to the task of securing the homeland. The Strategy also describes four foundations—unique American strengths that cut across all of the mission areas, across all levels of government, and

across all sectors of our society. These foundations—law, science and technology, information sharing and systems, and international cooperation—provide a useful framework for evaluating our homeland security investments across the federal government.

**Organizing for a Secure Homeland**

In response to the homeland security challenge faced by U.S., the Department of Homeland Security was established to ensure greater accountability over critical homeland security missions and unity of purpose among the agencies responsible for them.

**U.S. Department of Homeland Security**



Source: Department of Homeland Security

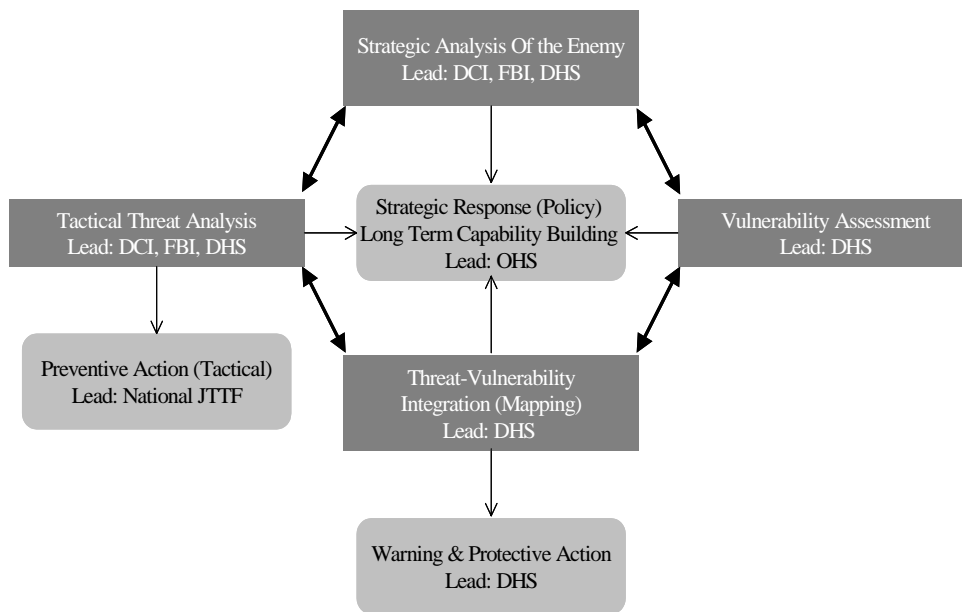
State and local governments have critical roles to play in homeland security. Indeed, the closest relationship the average citizen has with government is at the local level. State and local levels of government have primary responsibility for funding, preparing, and operating the emergency services that would respond in the event of a terrorist attack. Local units are the first to respond, and the last to leave the scene. All disasters are ultimately local events.

The private sector—the Nation’s principal provider of goods and services and owner of 85% of our infrastructure—is a key homeland security partner. It has a wealth of information that is important to the task of protecting the United States from terrorism. Its creative genius will develop the information systems, vaccines, detection devices, and other technologies and innovations that will secure our homeland.

## Issues Dealt by Homeland Security

### INTELLIGENCE AND WARNING

America’s intelligence community has made significant contributions to its national security and is now making adjustments to help meet the increased needs for homeland security. The National Strategy for Homeland Security reflects the concept that intelligence and information analysis is not a separate, stand-alone activity but rather an integral component of the Nation’s overall effort to protect against and reduce its vulnerability to terrorism. The basic roles and responsibilities in this Strategy are depicted below:



*Source: Office of Homeland Security*

This framework recognizes four interrelated but distinct categories of intelligence and information analysis, as well as three broad categories of actions that can follow from this analysis.

Tactical threat analysis: Actionable intelligence is essential for preventing acts of terrorism. The timely and thorough analysis and dissemination of information about terrorists and their current and potential activities allow the government to take immediate- and near-term action to disrupt and prevent terrorist acts and to provide useful warning to specific targets, security and public safety professionals, or the general population.

Strategic analysis of the enemy: The intelligence agencies need to have a deep understanding of the organizations that may conduct terrorist attacks against the United States. Knowing the identities, financial and political sources of support, motivation, goals, current and future capabilities, and vulnerabilities of these organizations will assist in preventing and preempting future attacks, and in taking long-term actions that can weaken support for organizations that seek to damage U.S. interests. Intelligence agencies can support the long-term U.S. strategies to defeat terrorism by understanding the roots of terrorism overseas, and the intentions and capabilities of foreign governments to disrupt terrorist groups in their territories and to assist the United States.

Vulnerability assessments: Vulnerability assessments are an integral part of the intelligence cycle for homeland security issues. They allow planners to project the consequences of possible terrorist attacks against specific facilities or different sectors of the economy or government. These projections allow authorities to strengthen defenses against different threats. Such assessments are informed by the use of tools such as computer modeling and analysis.

Threat-Vulnerability integration: Mapping terrorist threats and capabilities—both current and future against specific facility and sectoral vulnerabilities allows authorities to determine which organizations pose the greatest threats and which facilities and sectors are most at risk. It also allows planners to develop thresholds for preemptive or protective action.

***Three broad categories*** of action that can result from this analysis are below:

Tactical preventive action: Analysis can, and must, be turned into action that prevents terrorists from carrying out their plots. The United States has at its disposal numerous tools that allow for the disruption of terrorist acts in the United States and the detention of the terrorists themselves. These tools can be deployed as soon as the analysis uncovers evidence of terrorist planning. This analysis and assessment will help support and enable the actions taken by the U.S. government to prevent terrorism.

Warning and protective action: Inclusive and comprehensive analysis allows the government to take protective action, and to warn appropriate sectors and the public. Defensive action will reduce the potential effectiveness of an attack by prompting relevant sectors to implement security and incident management plans. In addition, defensive action works as a deterrent to terrorists weighing the potential effectiveness of their plans. Warnings allow entities and citizens to take appropriate actions to meet the threat, including upgrading security levels in any affected sectors, activating emergency plans, dispatching state and local law enforcement patrols, and increasing citizen awareness of certain activities.

Strategic response (policy): There is a need to develop and create new capabilities specifically designed to defeat the enemy of today and the enemy of the future. This immediate- and long-term strategic capability building will be shaped through budgetary allocations, and will be informed by the careful analysis and assessment of homeland

security information. Understanding terrorist organizations will allow policymakers to fashion policies that build international coalitions against terrorism, and eliminate sources of support or sanctuary for terrorists.

***Initiatives:***

- Enhance the analytic capabilities of the FBI
- Build new capabilities through the Information Analysis and Information Protection Division of the Department of Homeland Security
- Implement the Homeland Security Advisory System
- Utilize dual-use analysis to prevent attacks
- Employ "red team" techniques

**BORDER AND TRANSPORTATION SECURITY**

The United States shares a 5,525 mile border with Canada and a 1,989 mile border with Mexico. All people and goods legally entering into the United States are processed through an air, land, or sea port of entry. Many international airports are dispersed throughout the United States. Each year, more than 500 million people legally enter the country. Some 330 million are non-citizens; more than 85 percent enter via land borders, often as daily commuters. An enormous volume of trade also crosses our borders every day some \$1.35 trillion in imports and \$1 trillion in exports were processed in 2001.

America historically has relied heavily on two vast oceans and two friendly neighbors for border security, and on the private sector for most forms of domestic transportation security. The increasing mobility and destructive potential of modern terrorism has required the United States to rethink and rearrange fundamentally its systems for border and transportation security.

***Initiatives:***

- Ensure accountability in border and transportation security
- Create "smart borders" through border management system
- Increase the security of international shipping containers
- Implement the Aviation and Transportation Security Act of 2001
- Recapitalize the U.S. Coast Guard
- Reform immigration services

**DOMESTIC COUNTERTERRORISM**

The attacks of September 11 and the catastrophic loss of life and property that resulted have redefined the mission of federal, state, and local law enforcement authorities. While law enforcement agencies continue to investigate and prosecute criminal activity, they will now assign priority to preventing and interdicting terrorist activity within the United States.

The federal government has already instituted initiatives that have increased information sharing and the coordination of operations throughout the law enforcement community. Not only are the federal law enforcement and U.S. intelligence agencies communicating better with each other, the entire law

enforcement community—international, federal, state, and local—is now sharing more information. In addition, law enforcement agencies at all levels of government have worked to enhance coordination of their counterterrorism operational activities so that the collective efforts complement each other.

While the intelligence and law enforcement communities have made progress in the areas of information sharing and coordination, major shortcomings continue to exist in other important areas. The government's ability to identify key sources of funding for terrorist activity and the methods used to finance terrorist operations remains inadequate. The U.S. government has not yet developed a satisfactory system to analyze information in order to predict and assess the threat of a terrorist attack within the United States. The federal government needs to do a better job of utilizing the distinct capabilities of state and local law enforcement to prevent terrorism by giving them access, where appropriate, to the information in our federal databases, and by utilizing state and local information at the federal level. The FBI-led Joint Terrorism Task Forces, by including participants from state and local law enforcement as well as federal agencies, draw on state and local capabilities, and enhance intergovernmental coordination.

### ***Initiatives:***

- Improve intergovernmental law enforcement coordination
- Facilitate apprehension of potential terrorists
- Continue ongoing investigations and prosecutions
- Complete FBI restructuring to emphasize prevention of terrorist attacks
- Target and attack terrorist financing
- Track foreign terrorists and bring them to justice

## **PROTECTING CRITICAL INFRASTRUCTURE AND KEY ASSETS**

Protecting America's critical infrastructure and key assets is a formidable challenge. The country's open and technologically complex society presents an almost infinite array of potential targets, and our critical infrastructure changes as rapidly as the marketplace. It is impossible to protect completely all targets, all the time. On the other hand, Homeland security can help deter or deflect attacks, or mitigate their effects, by making strategic improvements in protection and security. Thus, while Homeland security cannot assume it will prevent all terrorist attacks, it can substantially reduce America's vulnerability, particularly to the most damaging attacks.

The USA PATRIOT Act defines critical infrastructure as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." U.S. critical infrastructures are particularly important because of the functions or services they provide to the country. The critical infrastructures are also particularly important because they are complex systems: the effects of a terrorist attack can spread far beyond the direct target, and reverberate long after the immediate damage.

America's critical infrastructure encompasses a large number of sectors. These include:

- Agriculture
- Food

- Water
- Public Health
- Emergency Services
- Government
- Defense Industrial Base
- Information and Telecommunications
- Energy
- Transportation
- Banking and Finance
- Chemical Industry
- Postal and Shipping

Protecting America's critical infrastructure and key assets requires more than just resources. The federal government can use a broad range of measures to help enable state, local, and private sector entities to better protect the assets and infrastructures they control. For example, the government can create venues to share information on infrastructure vulnerabilities and best practice solutions, or create a more effective means of providing specific and useful threat information to non-federal entities in a timely fashion.

In addition to the country's critical infrastructure, the country must also protect a number of key assets—individual targets whose destruction would not endanger vital systems, but could create local disaster or profoundly damage the Nation's morale or confidence. Key assets include symbols or historical attractions, such as prominent national, state, or local monuments and icons. In some cases, these include quasi-public symbols that are identified strongly with the United States as a Nation, and fall completely under the jurisdiction of state and local officials or even private foundations. Key assets also include individual or localized facilities that deserve special protection because of their destructive potential or their value to the local community.

***Initiatives:***

- Unify America's infrastructure protection effort in the Department of Homeland Security
- Building and maintain a complete and accurate assessment of America's critical infrastructure and key assets.
- Enable effective partnership with state and local governments and the private sector.
- Develop a national infrastructure protection plan
- Securing cyberspace
- Harness the best analytic and modeling tools to develop effective protective solutions
- Guard America's critical infrastructure and key assets against "inside" threats
- Partner with the international community to protect country's transactional infrastructure

## • DEFENDING AGAINST CATASTROPHIC THREATS

Currently, chemical, biological, radiological, and nuclear detection capabilities are modest and response capabilities are dispersed throughout the country at every level of government. Responsibility for chemical, biological, radiological, and nuclear surveillance as well as for initial response efforts often rests with state and local hospitals and public health agencies. Today, if a natural disaster or terrorist attack causes medical consequences that exceed local and state capabilities, the Department of Health and Human Services would coordinate the deployment of medical personnel, equipment, and pharmaceuticals among the Departments of Agriculture, Defense, Energy, Justice, Transportation, Veterans Affairs, the Environmental Protection Agency, the Federal Emergency Management Agency, General Services Administration, National Communications System, U.S. Postal Service, and the American Red Cross.

While the government's collaborative arrangements have proven adequate for a variety of natural disasters, the threat of terrorist attacks using chemical, biological, radiological, or nuclear weapons with potentially catastrophic consequences demands new approaches, a focused strategy, and a new organization. The country has already expanded capabilities and improved coordination among federal agencies, but more can be done to prepare and respond.

### *Initiatives:*

- Prevent terrorist use of nuclear weapons through better sensors and procedures
- Detect chemical and biological materials and attacks
- Improve chemical sensors and decontamination techniques
- Develop broad spectrum vaccines, antimicrobials and antidotes
- Harness the scientific knowledge and tools to counter terrorism

## EMERGENCY PREPAREDNESS AND RESPONSE

Under the President's proposal, the Department of Homeland Security, building on the strong foundation already laid by the Federal Emergency Management Agency (FEMA), will lead the national efforts to create and employ a system that will improve nation's response to all disasters, both manmade and natural.

Many pieces of this national emergency response system are already in place. America's first line of defense in the aftermath of any terrorist attack is its first responder community—police officers, firefighters, emergency medical providers, public works personnel, and emergency management officials. Nearly three million state and local first responders regularly put their lives on the line to save the lives of others and make our country safer. These individuals include specially trained hazardous materials teams, collapse search and rescue units, bomb squads, and tactical units.

In a serious emergency, the federal government augments state and local response efforts. FEMA, which under the President's proposal will be a key component of the Department of Homeland Security, provides funding and command and control support.

***Initiatives:***

- Integrated separate federal response plans into a single all discipline incident management plan
- Create a national incident management system
- Improve tactical counterterrorist capabilities
- Enable seamless communication among all responders
- Prepare health care providers for catastrophic terrorism
- Augment America's pharmaceutical and vaccine stockpiles
- Prepare for chemical, biological, radiological, and nuclear decontamination
- Plan for military support to civil authorities
- Build a national training and evaluation system
- Enhance the victim support system