Chapter 2

Introduction to Homeland Security

Statutory Authority

**Pre-9/11**

- Legislation to deal with terrorist threats began long before 9/11, **but:**
  - Support was weak
  - Federal institutional culture a barrier to change
  - Terrorism authorities were vague and not well established
  - 9/11 brought about a complete reversal

**Pre-9/11**

- Several terror events occurred during Clinton’s first 3 years in office:
  - 1993 Bombing of the World Trade Center
  - 1995 Oklahoma City Bombing
  - 1995 Tokyo Subway Sarin Gas Attacks
**Pre-9/11: Nunn-Lugar-Domenici Act**

- Attacks prompted the drafting and passage of the Nunn-Lugar-Domenici WMD Act
  - Primary result - provision of greater funding for training and equipment for first responders
  - Act addressed response to terrorist attack, *but not prevention*

**Pre-9/11: Federal Response Plan (FRP) - Terrorism Annex**

- 1996 Atlanta Olympics bombing
  - Attack source was domestic
  - Helped to drive the development of a Terrorism Annex to the FRP
  - Annex addressed criminal element in terrorist attack response
    - Had confounded previous responses to terrorism
    - Was recognized as needing special consideration
  - Laid out inter-agency coordination in response to future attacks

**The Three Commissions**

1) Hart-Rudman Commission

  - Goal: Design a national security strategy for domestic terrorism
  - Recommendation: Create a National Homeland Security Agency responsible for planning, coordinating, and integrating federal activities
    - Responsible for safety of American people
    - Oversee protection of critical infrastructure (to include information technology)
  - Commission’s recommendations largely ignored
The Three Commissions
2) Gilmore Commission

- The Gilmore Commission
  - Produced series of annual reports between 1999 and 2003
  - Presented a growing base of knowledge concerning the Weapons of Mass Destruction (WMD) risk
  - Recommended a course of action to counter that risk

The Three Commissions
3) Bremer Commission

- The Bremer Commission (aka - National Commission on Terrorism)
  - Addressed international terrorist threat
  - Evaluated laws, policies, and practices for:
    - Preventing terrorism
    - Punishing terrorists
  - Produced “Countering the Changing Threat of International Terrorism” report in 2000

The Three Commissions
3) Bremer Commission (cont.)

- "Countering the Changing Threat of International Terrorism" report concluded the following:
  - International terrorism poses an increasing threat to US
  - Countering that threat required significantly stepping up US efforts
  - #1 priority was to prevent terrorist attacks
  - US policies must firmly target states that support terrorists.
  - Private and logistical support must be prosecuted
  - Terrorist attacks involving WMD could profoundly affect the entire nation
  - President and Congress should review system for reviewing and funding CT programs
**The Three Commissions**

- Despite each commission’s conclusions and recommendations, no major programs were initiated to combat the growing risk
  - Lack of recognition of a terrorist threat within the country’s borders contributed to inaction

---

**Presidential Decision Directive (PDD) 62 - May 1998**

- PDD-62: “Combating Terrorism”
  - Called for the establishment of the Office of the National Coordinator for Security, Infrastructure Protection, and Counterterrorism
  - **Goal**: create systematic approach to fighting terrorism
  - Tasked with overseeing a broad variety of policies and programs to include:
    - Counter-terrorism (CT)
    - Critical infrastructure protection
    - WMD preparedness
    - Consequence management

---

**Presidential Decision Directive (PDD) 63**

- PDD-63: “Protecting America’s Critical Infrastructure”
  - Tasked all Federal departments with:
    - Assessing the vulnerabilities of their cyber and physical infrastructures, and;
    - To work to reduce their exposure to new and existing threats
**AG’s 5-Year Interagency Plan**

  - FBI emerged as the principal counter-terror agency for response and investigation
  - Plan represented a substantial inter-agency effort
  - Recommended specific agency action to help resolve interagency issues
  - But plan failed to tear down the walls that prevented interagency sharing of information

**Govt. Accounting Office (GAO) Findings**

- GAO reviewed PPD’s and AG 5-yr Plan and concluded that a comprehensive national security strategy was lacking
  - No measurable outcomes
  - Lacked goals for improvement of state/local responsibilities
  - No single entity acting as top federal official accountable to both the POTUS and Congress for terrorism hazard
  - No coordination in domestic preparedness programs and the development of a national strategy

**GAO Findings (cont.)**

- Federal Government ill-equipped and unprepared to counter a major terrorist attack
- From sharing intelligence to coordinating a response, the government had failed to put in place an effective critical infrastructure system
GAO Findings (cont.)

- To prevent terrorist attacks the GAO recommended:
  - A national strategy to combat terrorism and computer-based attacks
  - Better protection for the nation’s infrastructure
  - A single focal point to oversee coordination of federal programs

GAO Findings (cont.)

- To prevent terrorist attacks the GAO recommended:
  - Completion of a threat assessment of likely WMD and other weapons that might be used by terrorists
  - Revision of the AG’s 5-Year Interagency Counterterrorism and Technology Crime Plan to better serve a national strategy
  - Coordination of research and development to combat terrorism

9/11 Attacks

- The first truly national disaster event
- First disaster that impacted all Americans
- Left all citizens with a sense of vulnerability
- Economic consequences felt worldwide
- Almost 3,000 people killed, and billions of dollars in property damage resulted
9/11 Attacks (cont.’d)

- Full economic impacts may never be known
- Many instances where the attacks could have been prevented
- Insufficient interagency coordination prevented Federal Government from piecing together the larger picture of what exactly was occurring

9/11 - Immediate Response

- Sept. 20th - President Bush announced that an Office of Homeland Security would be established in the White House, as well as a Homeland Security Council, by executive order
  - PA Governor Ridge Tom Ridge to be director
- Sept. 24th - President Bush announced that he will be seeking passage of the “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act” (USA PATRIOT Act of 2001)

9/11 - Immediate Response (cont.’d)

- Oct. 8th - President Bush signed executive order creating Office of Homeland Security
- Oct. 26th - President Bush signed USA PATRIOT Act into law after little deliberation in Congress
- Oct 29th - President Bush issued first of many Homeland Security Directives (HSDs)
The “USA PATRIOT” Act

- Introduced to deter and punish terrorist acts and to enhance law enforcement investigatory tools
- Principle focus is:
  - To provide law enforcement authorities with the proper legal authority to collect information on suspected terrorists
  - To detain those suspected of being or aiding terrorists
  - To deter terrorists from entering and operating within the US
  - To limit terrorist money laundering

The “USA PATRIOT” Act

- Major provisions:
  - Relaxes restrictions on info sharing between law enforcement and intelligence agencies
  - Makes it illegal to knowingly harbor a terrorist
  - Authorizes roving wiretaps
  - Allows US govt. to detain non-citizens suspected of terrorism for up to 7 days w/o specific charges
  - Greater govt. access to e-mail records
  - Triples number of border patrol, customs inspectors, and INS inspectors at the northern US border
  - Eliminates statute of limitations for the most serious terrorist acts

The “USA PATRIOT” Act (cont.)

- Act passed with little deliberation
- Sparked concern over the protection of civil rights
  - Govt. powers have been expanded without corresponding appropriate checks and balances
- DOJ countered that authority was necessary to effectively track and detain terrorists
- Numerous communities have passed resolutions opposing part or all of the act’s contents
The “USA PATRIOT” Act (cont.)

- Act contained many sunset provisions
  - Portions of the Act were set to expire on 31 DEC 2005
- PATRIOT Act reauthorized under two separate bills
  - USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005
    - Passed by Congress in July 2005
  - USA PATRIOT Act Additional Reauthorization Amendments of 2006
    - Passed by Congress in February 2006
    - Both signed into law 6 MAR 2006

The “USA PATRIOT” Act (cont.)

- 27 FEB 2010: Pres. Obama signed into law legislation extending three provisions of the Patriot Act for one year
  - Authorizes court-approved roving wiretaps that permit surveillance on multiple phones
  - Authorizes court-approved seizure of records and property in anti-terrorism operations
  - Permits surveillance of “lone wolf” terrorists

Foreign Intelligence Surveillance Act (FISA) – A Brief Background

- Passed in 1978 following Watergate and revelations about the systematic surveillance of journalists and political opponents of the govt.
- Set forth the procedures for the conduct of electronic surveillance and physical searches for foreign intelligence purposes
- FISA also authorized a special federal FISA Court (FISC) to regulate and monitor the executive branch’s conduct
FISA – A Brief Background (cont.)

- Designed to ensure that prosecutors and criminal investigators did not use FISA to circumvent more rigorous warrant requirements for criminal investigations
  - Criminal investigations must present probable cause to obtain a warrant
  - FISA is not principally about crime, it is about national defense
  - But reality is that national security issues and criminal acts are often inter-related, regardless of the original investigative intent

FISA – A Brief Background (cont.)

- Over the years the Dept. of Justice (DOJ) interpreted FISA rules to mean that the use of FISA was restricted when a law enforcement investigation was involved
  - Former AG Janet Reno issued internal guidelines solidifying this interpretation
  - Thus, internal DOJ procedures created a “wall” inhibiting coordination of these types of investigations and the sharing of information.
  - Limited the use of FISA evidence in criminal cases unless govt. could demonstrate that the primary purpose of the investigation was intel collection

FISA – A Brief Background (cont.)

- Aug 2001:
  - FBI Headquarters declined to allow criminal investigators to assist an intelligence investigation seeking to locate probable terrorists Khalid al-Midhar and Nawaf al-Hazmi
  - A few weeks later, the pair helped hijack Flight 77 and pilot it into the Pentagon
Fourth Amendment to the US Constitution

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

- Must have probable cause to make an arrest
- Must have probable cause to conduct a search

Probable Cause

- A reasonable belief that a person has committed a crime
  - Would the facts and circumstances lead a prudent person to believe that a suspect has committed, is committing, or is about to commit a crime?
  - More than articulable suspicion, but less than that required to secure a conviction

Problem

- How should we deal with terrorism?
  - Is it a crime, to be dealt with by law enforcement?
  - Or is it a national security matter more akin to fighting a war?
The “USA PATRIOT” Act - Section 218: Amending the FISA Standard

Changes the certification requirement when the govt. seeks a FISA surveillance or search order

- Previously, the govt. was required to certify that “the purpose” of the application was to obtain foreign intelligence information
- Now, govt. must certify that obtaining foreign intelligence information is “a significant purpose” of the application
- 218 was intended to clarify that no such separation between criminal and intelligence investigations was necessary

Criticisms against:

- Alleged FISA “wall” never existed.
  - Info-sharing an administrative and bureaucratic problem, not statutory
- Unconstitutional
  - Permits searches undertaken primarily for criminal law purposes on less than the probable cause required under the Fourth Amendment
  - Requires Govt. to show probable cause that the target of the search is an “agent of a foreign power”, not that evidence of a crime will be found
  - Definition of “foreign agent” too broad
- If an investigation turns primarily criminal in nature, govt. should be required to obtain criminal warrants

Support for:

- Eliminates the reason for misinterpretation of the FISA rules
- Prone to abuse claims unfounded
  - Easier to fabricate evidence necessary to get a criminal warrant than to dishonestly use FISA to get info
- Not a lower showing of suspicion—a different showing of suspicion
  - Still requires probable cause of a foreign power/agency vice traditional crime
### The “USA PATRIOT” Act - Sections 203 and 905: Authority to Share Criminal Investigative Information

- Addressed perceived legal barriers in the Foreign Intelligence Surveillance Act (FISA) that limited law enforcement agencies from sharing information with intelligence agencies.
- Allows the sharing of information that is in any way related to any American’s contact with any foreign government, group, or individual.
  - Applies to:
    - All intercepts of telephone conversations and
    - All confidential information obtained by a grand jury.
  - Requires federal law enforcement to disclose all foreign intelligence acquired during law enforcement investigations.

### The “USA PATRIOT” Act - Sections 203 and 905: Authority to Share Criminal Investigative Information

**Criticisms against:**
- Does not limit info sharing to officials with responsibility for terrorism.
- Does not limit info sharing to info related to terrorism.
- No safeguards for the subsequent use or dissemination of the info.

**Support for:**
- Often difficult to determine what info is related to terrorism.
- Clears up confusing restrictions on sharing information.

### The “USA PATRIOT” Act - Section 206: Roving Surveillance Authority Under FISA

- Addressed the need to obtain a warrant to tap each device a target used.
- Allows the Foreign Intelligence Surveillance Court (FISC) to order “roving” or multi-point surveillance.
  - Focus is now on the target vice the device.
  - Brings FISA rules more in line with criminal wiretap laws.
    - However, unlike the criminal laws, it does not require the government to “ascertain” where the targeted communication will take place before intercepting communications.
    - Also, govt. need not ID target if ID unknown.
The “USA PATRIOT” Act - Section 206: Roving Surveillance Authority Under FISA

Criticisms against:
- Open for abuse - Allows surveillance of “anyone, anywhere” (John Doe warrants)
- Lacks ascertainment requirement (only conduct intercept when target is using the device)
- No requirement to ID either the target or the location (phone number, internet account, etc.) of the intercept
- Thus violates 4th Amendment requirement
  - All warrants must “particularly describe the place to be searched”

The “USA PATRIOT” Act - Section 206: Roving Surveillance Authority Under FISA

Support for:
- Statute already has safeguards against misconduct
  - Authorization for intercept must be based on probable cause that:
    - The target is a foreign power or an agent of a foreign power
    - Each of the facilities or places where the surveillance is directed is being used or will be used
  - Minimization - Requires the termination of surveillance upon the determination that the intercepted conversation is innocent
- Terrorism investigations should not be subject to the same rules as criminal investigations

The “USA PATRIOT” Act - Sections 209, 212, and 220: Access to Wire and Electronic Communications

Section 209
- Previously, seizure of stored voicemail required a court order that had more stringent requirements than a criminal search warrant
- Stored e-mail only required an ordinary search warrant or a subpoena
- Section 209 applies same rules to stored voicemail as for stored e-mail
The “USA PATRIOT” Act - Sections 209, 212, and 220: Access to Wire and Electronic Communications

Criticisms against 209:
- When voicemail stored on a home answering machine is seized, owner is notified immediately
  - You can examine the warrant and assert your rights
- When e-mail is seized from a service provider, you might not be provided notice until trial
- If you were mistakenly targeted, you need not be told.

The “USA PATRIOT” Act - Sections 209, 212, and 220: Access to Wire and Electronic Communications

Section 212
- Electronic privacy laws prohibit service providers from voluntarily disclosing, even to the govt., most customer communications or records
- Section 212 allows providers to disclose this material if they “reasonably believe” that there is “an emergency involving immediate danger of death or physical injury to any person”

The “USA PATRIOT” Act - Sections 209, 212, and 220: Access to Wire and Electronic Communications

Criticisms against 212:
- Once access is granted, it is no longer subject to judicial approval
- No time limits on the period covered
- No minimization requirement
- No report back to a judge
- No requirement to notify the person surveilled (unless and until govt. introduces at a trial)
- Govt. could exaggerate the “emergency” to convince a service provider to disclose the records
The “USA PATRIOT” Act - Sections 209, 212, and 220: Access to Wire and Electronic Communications

Section 220
- Previously, the govt. could only seek a search warrant for service providers' customer communications/records in the jurisdiction where the service provider was located
- Often times, providers are not located where the crime occurs
- Section 220 allows the court in the district where the crime occurs to issue search warrants to be served anywhere in the country

Criticisms against 220:
- Makes it more difficult for a service provider to appear before the issuing court and object to legal or procedural defects

Support for 209, 212, and 220:
- Corrects problems in the 1986 Electronic Communications Protection Act (ECPA)
  - Lack of exigent circumstances exception
  - Unopened voice-mail required a “super-warrant Title III wire-tapping order”; opened voice-mail required nothing more than a simple subpoena
  - Created unnecessary delays by district restrictions on obtaining court orders
- Current rule in criminal investigations does not require notice of access to records
  - Notice could tip off a suspect and thwart an investigation

...
**The “USA PATRIOT” Act - Sections 213: “Sneak and Peek” Search Warrants**

- Authorizes delayed notice of the execution of search warrants for intangible items (for any federal crime, not just terrorism cases)
  - Govt. must show “reasonable cause” to believe that providing notice of a search would have an adverse affect
    - Endanger a person’s life or physical safety
    - Flight from prosecution
    - Destruction of or tampering with evidence
    - Intimidation of a potential witness
    - Otherwise jeopardizing an investigation or unduly delaying a trial

- 213 warrants prohibit the seizure of any tangible property, any wire or electronic communication, or any stored wire or electronic information, except where the court finds reasonable necessity for the seizure

- Support for:
  - Federal investigators have already had this power for decades for investigations related to drugs, organized crime, and child pornography
  - Delay must be approved by a judge
  - Requires notification after a reasonable amount of time
The “USA PATRIOT” Act
Sections 213: “Sneak and Peek” Search Warrants

- Criticism against:
  - 213 not limited to terrorism cases
  - “Adverse result” and “reasonable time” not sufficiently defined

The “USA PATRIOT” Act
Sections 214: Pen Register and Trap and Trace Authority; 215: Access to Business Records Under FISA (Libraries Provision)

- Section 215:
  - Eliminates any limitations on the types of businesses or entities whose records may be seized
  - Previously, FISA rules only permitted seizure of records of hotels, motels, car and truck rental agencies and storage rental facilities
  - Also broadens authority from “records” to “any tangible things (including books, records, papers, documents, and other items)”

The “USA PATRIOT” Act
Sections 214: Pen Register and Trap and Trace Authority; 215: Access to Business Records Under FISA (Libraries Provision)

- Section 215 (cont.):
  - Eases requirements for obtaining orders to seize business records
  - Previously, FISA required the FBI to provide “specific articulable facts giving reason to believe” that the subject of an investigation was a “foreign power or the agent of a foreign power”
  - New govt. is only required to assert that the records or things are sought for a foreign intelligence investigation or to protect against international terrorism or clandestine intelligence activities (except 1st Amendment activities)
  - No requirement for an evidentiary or factual showing
    - Judge must issue the order if application meets requirements
Section 214:
- Previously, FISA required the govt. to certify that there was reason to believe that the monitored line would be used by someone engaged in:
  - International terrorism
  - Spying
- Certificate requirements now similar to that of Section 215

Criticism against 214, 215:
- 215 trumps other laws that govern the release of records, e.g. – medical records, generally subject to privacy expectations
- Lowers the standard to obtain records; raises possibility of abuse—could lead to routine surveillance
- 215 contains a “gag rule”
  - “No person shall disclose to any other person (other than those persons necessary to produce the tangible object) that the FBI has sought or obtained tangible things under this section.”
  - “Gag rule” an unjustified expansion of a special rule for wiretaps and is contrary to the rules that have applied to govt. requests for records.

Support for 214, 215:
- Brought FISA in line with what could already be compelled via subpoena in criminal investigations
- Criminal subpoenas not subject to judicial review, so neither should 215 requests
  - When neither US persons nor legitimate expectations of privacy are not involved, court has no cause to demand an explanation
- 214 extends to e-mail and internet what is already extended to telephones
- Stakes in a terrorism investigation potentially much higher than a criminal investigation if a suspect is tipped off
Section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004: aka The “Lone Wolf” Amendment

- Amends FISA’s definition of “an agent of a foreign power” to include any person, other than a US person, who “engages in international terrorism or activities in preparation therefore.”
- Previous FISA definitions did not cover unaffiliated individuals (“lone wolves”)

Thus a target can be considered an “agent of a foreign power” without any evidence that they are acting with a group

But, govt. must present probable cause that the target is engaging or preparing to engage in “international terrorism”

International terrorism defined as:

- Violent criminal acts;
- Intended to intimidate or coerce a population or govt. and;
- That occur totally outside of the US or transcend national boundaries

The USA PATRIOT Improvement and Reauthorization Act

- Signed into law by President Bush on 9 MAR 2006
- Modified the USA PATRIOT Act as follows:
  - Made permanent 14 of the 16 expiring PATRIOT Act sections
  - Creates new sunset of 31 DEC 2009 for sections 206 (“roving” FISA wiretaps) and 215 FISA requests for business records
The USA PATRIOT Improvement and Reauthorization Act (cont.)

Section 213 Changes:
- Notice of the search must be given no more than 30 days after the execution of the search
- 90 extension may be granted if the facts of the case justify
- Removed “unduly delaying a trial” as one of the “adverse consequences”
- A detailed annual report must be submitted annually to Congress regarding the use and number of warrants authorizing delayed notice

The USA PATRIOT Improvement and Reauthorization Act (cont.)

Section 215 Changes:
- AG must submit to Congress an annual report regarding the use of this section
- Total number of applications
- Total number of orders granted as requested, granted as modified, or denied
- Number of orders granted, modified or denied for each of the following:
  - Library circulation records and patron lists
  - Book sales records/customer lists
  - Firearms sales records
  - Tax return records
  - Educational records
  - Medical records

The USA PATRIOT Improvement and Reauthorization Act (cont.)

Section 215 Changes (cont.):
- Applications for 215 orders for the following records requires approval by the FBI Director, the FBI Deputy Director, or the Executive Asst. Dir. for National Security:
  - Library
  - Bookstore
  - Firearm sales
  - Tax returns
  - Educational
  - Medical
The USA PATRIOT Improvement and Reauthorization Act (cont.)

Section 215 Changes (cont.):
- Requires AG to establish standards for the collection and dissemination of info obtained via a 215 order (minimization)
  - May not disclose such info except for lawful purposes

Section 215 Changes (cont.):
- Establishes a detailed judicial review process
  - Recipients of 215 orders may challenge the legality of the order before a FISA judge
- Expands the list of gag order exceptions
  - 215 order recipient can now consult with an attorney and does not have to identify that person
- Allows recipient to challenge the non-disclosure order after one year

Section 215 Changes (cont.):
- Before, 215 application only needed to state that the records were being sought for an authorized investigation
- Now, application must include a “statement of facts” demonstrating that there are reasonable grounds to believe that the tangible items sought are “relevant” to an authorized or preliminary investigation to protect against international terrorism or to obtain foreign intelligence not concerning a US person
**The USA PATRIOT Improvement and Reauthorization Act (cont.)**

- **Section 215 Changes (cont.):**
  - Application must also show that the items sought pertain to:
    - a foreign power or an agent of a foreign power,
    - the activities of a suspected agent of a foreign power who is the subject of such authorized investigation or,
    - an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation

---

**The USA PATRIOT Improvement and Reauthorization Act (cont.)**

- **Section 206 Changes:**
  - Application must describe the specific target if the target's identity is unknown
  - If the govt. begins to monitor a new place or facility that was not contained in the original order, the govt. must notify the FISA court within 10 days of the change

---

**National Security Letters (NSLs)**

- Authorize federal intelligence investigators to request that communications providers, financial institutions, and credit bureaus provide certain types of customer business records, including subscriber and transactional info related to Internet and telephone usage, credit reports, and financial records
- Similar to 215 orders except:
  - Do not need prior approval from a judge
  - Can be used only to receive "non-content information", e.g. - phone number called or e-mail address used
**NSLs - Doe v. Ashcroft**

- A federal court in the Southern District of NY has held that the FBI’s practices and procedures regarding NSLs violates the Fourth and First Amendments (Sep 2004)
  - Lack of judicial review before or after the issuance of a NSL
  - NSL gag order requirements
- USA PATRIOT Improvement and Reauthorization Act now allows a NSL recipient to challenge both the NSL and the gag order

**National Security Letters (NSLs)**

- USA PATRIOT Improvement and Reauthorization Act also now requires that before a gag order may be imposed, that the requesting agency must certify that any disclosure may:
  - Endanger any individual or the national security of the US
  - Interfere with diplomatic relations
  - Or interfere with a criminal or intelligence investigation
- Thus, a gag order does not automatically attach to an NSL like it does under a 215 order
- Disclosure may also be made to comply with the NSL or to obtain legal advice from an attorney
- NSL not applicable to libraries

**Homeland Security Act of 2002**

- Signed into law by President George W. Bush on November 25, 2002
- Provided authorization for the establishment of the Department of Homeland Security (DHS)
- Established DHS as an executive branch agency, with the DHS Secretary reporting directly to the President
- Outlined the DHS management structure
Homeland Security Act of 2002 (cont.)

- Identified those agencies and programs to be migrated to DHS
  - Secret Service
  - Coast Guard
- Called for the transfer of Bureau of Alcohol, Tobacco, Firearms, and Explosives (BATFE) from Treasury Dept. to DOJ
- Detailed the roles and responsibilities of the five directorates that comprise DHS
  - Information Analysis and Infrastructure Protection
  - Science and Technology
  - Border and Transportation Security
  - Emergency Preparedness and Response
  - Management

Homeland Security Act of 2002 (cont.)

- Also established the:
  - Homeland Security Council
    - Advises the president on homeland security matters
  - Office for State and Local Coordination and Preparedness
    - Reports to the DHS secretary

DHS Tasks

- Prevent terrorist attacks within the United States
- Reduce the vulnerability of the U.S. to terrorism
- Minimize the damage, and assist in the recovery, from terrorist attacks that occur within the U.S.
- Carry out all functions of transferred entities
- Ensure that the agencies’ functions that are not related directly to homeland security are not diminished or neglected
- Ensure that the overall economic security of the U.S. is not diminished by efforts, activities, and programs aimed at securing the homeland
- Monitor connections between illegal drug trafficking and terrorism, coordinate efforts to sever such connections
Homeland Security Presidential Directive (HSPD)-5

- Released on February 28, 2003 “to enhance the ability of the United States to manage domestic incidents”
- Tasked the DHS Secretary to develop and administer a National Incident Management System (NIMS) and a National Response Plan (NRP)

Homeland Security Presidential Directive (HSPD)-5 (cont.)

- National Incident Management System (NIMS)
  - Designed to integrate EM practices (mitigation, preparedness, response and recovery) of all govt. levels (federal, state, local) into a comprehensive national framework
  - Central mission is to enable responders at all levels to work together more effectively to manage domestic incidents, no matter what the size

Homeland Security Presidential Directive (HSPD)-5 (cont.)

- National Response Plan (NRP)
  - A single, comprehensive framework for the management of domestic incidents
  - Replaced Federal Response Plan (FRP)
  - NRP changed in Jan 2008 to the National Response Framework (NRF)
Post-Katrina Emergency Management Reform Act

- Established several new leadership positions within DHS
- Moved additional functions into or back to FEMA
- Created and reallocated functions to other DHS components
- Amended the Homeland Security Act in ways that directly/indirectly affected the organization and functions of the various entities within DHS

9/11 Commission

- Created by Congress to:
  - Allow for a full investigation into the 9/11 attacks
  - Make recommendations as to how such attacks can be prevented in the future
- Released on July 22nd, 2004
  - 37 recommendations to help prevent future terrorist attacks
- Divided into three subject areas:
  - 1) Attacking terrorists and their organizations
  - 2) Preventing the growth of Islamic terrorism
  - 3) Protecting against and preparing for terrorist attacks

9/11 Commission Report

- Proposed a five-part plan:
  1) Closing the foreign-domestic divide by linking intel and operational planning in a new National Counterterrorism Center
  2) Bringing the intel community together under a National Intelligence Director and national intelligence centers
  3) Encouraging info sharing throughout govt. through decentralized networks
  4) Centralizing and strengthening Congressional oversight of intel and homeland security issues
  5) Strengthening the national security workforce within the FBI and clarifying the missions of the DoD and DHS
Budget Appropriations

- DHS budget has steadily increased since 2003
  - FY 2003 - $29.8 billion
  - FY 2008 - $37.7 billion
  - FY 2009 - $50.5 billion
  - FY 2010 - $56.4 billion
- Costs may call into question DHS sustainability
  - Support for high costs may wane over time without more attacks
  - Some costs wholly unrelated to terrorism