NATIONAL SECURITY ORIENTATION

Law Enforcement And Intelligence Working Together To Meet The Challenges Of The 21st Century

July 2004

This National Security Orientation Power Point presentation is intended for use as a basic orientation for all personnel new to National Security, including prosecutors, law enforcement personnel and agents, analysts, and support staff, at the Department of Justice (DOJ), Federal Bureau of Investigation (FBI), and United States Attorneys' Offices (USAOs). The Orientation includes a number of Power Point slides divided into the following sections: Introduction to Terrorism; DOJ Strategy for Combating Terrorism; Organization; National Security Tools and Techniques; and Handling National Security Information.

Presentation Overview

- Section I: Introduction to National Security
  - Terrorism
  - Espionage and Counter Intelligence
- Section II: Department of Justice Strategy for Combating Terrorism
- Section III: DOJ National Security Components
- Section IV: National Security Tools and Techniques
- Section V: Handling National Security Information

Section I

Introduction to National Security

Introduction to Terrorism

- What is terrorism?
- What are the goals of terrorists?
- What methods do they use to achieve these goals?
- Why is modern international terrorism so threatening?
- What are the major terrorist groups?
- What are some examples of terrorist acts?

The first part of this presentation is a general introduction that includes a brief history of terrorism over the past two centuries and an overview of modern international terrorism. We will also discuss the methods, goals, and capabilities of terrorists; provide information on our strategy to combat them; list some of the major terrorists groups; and provide some examples of recent terrorist acts.

What is Terrorism?

- **Terrorism can be defined as the calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological;**

  or

- **Non-state political violence targeting noncombatants.**

There is no universally agreed upon definition of terrorism. It is difficult to arrive at one mutually acceptable definition for such a complex problem. For our purposes the above definitions of terrorism will suffice, but it is both interesting and important from a policy-making standpoint to keep in mind the difficulties of even clearly defining terrorism, let alone effectively combating it.

Statutory Basis

The U.S. Federal Criminal Code defines international terrorism as "activities that—

(A) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;

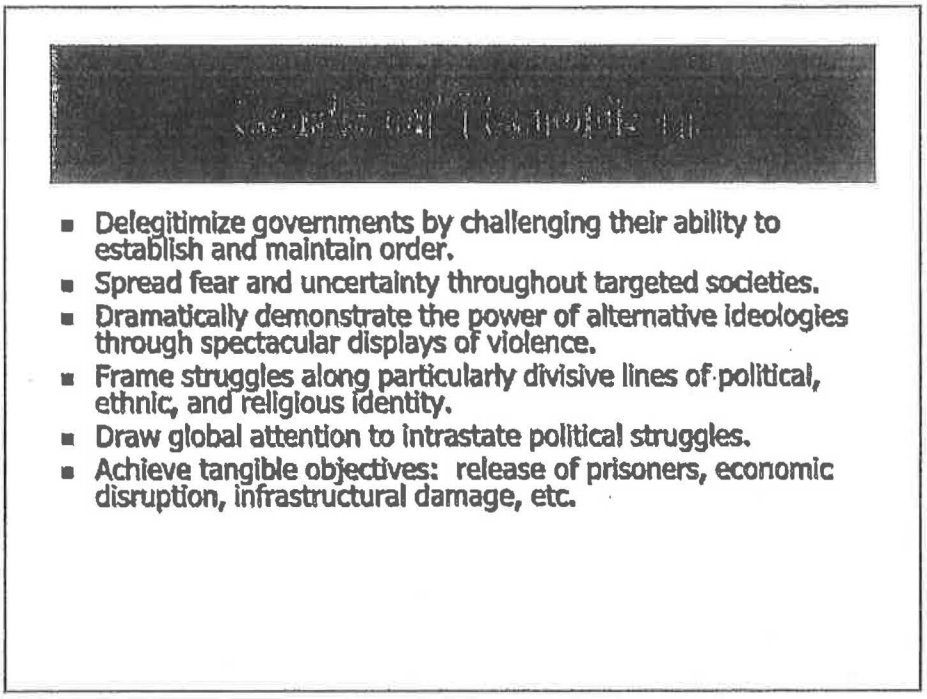
(B) appear to be intended-

(i) to intimidate or coerce a civilian population;

(ii) to influence the policy of a government by intimidation or coercion; or

(iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and

(C) occur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum." See 18 U.S.C. § 2331.



Terrorism can be used to serve a number of different ends. Some terrorists seek to violently deconstruct existing governments in order to establish new (and, in the terrorists' view, more just) political orders. Religiously inspired terrorist groups, such as Al Qaeda and certain white supremacist groups in the United States, most often fall under this category. Leftist terrorist groups, such as the Japanese Red Army, also tend to fall into this category of deconstructionists.

Other terrorist groups seek to gain political autonomy along ethnic/nationalist lines through violence, without necessarily seeking the total destruction of existing states. This type of terrorism typically occurs under one of two circumstances: 1) indigenous populations seeking to expel a foreign political presence and establish political autonomy and sovereignty for a native population; and 2) politically disenfranchised ethnic or religious groups living under regimes that under-represent their groups' distinct interests or conflict with their political, religious, or socioeconomic ideologies. Another objective of terrorists is to draw attention (and potential support) to their causes by forcing themselves on the world stage through dramatic displays of violence, such as plane hijackings and hostage-takings. Terrorists often also seek more tangible objectives from their attacks, such as the release of prisoners or the damage of property.

METHODS OF TERRORISM

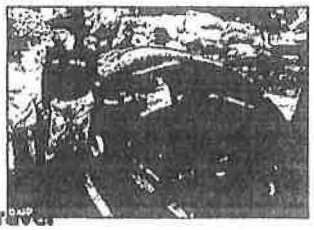
METHODS INCLUDE:

- Bombings
- Hostage Taking
- Sabotage
- Suicide Attacks
- Hijacking
- Arson
- Assault
- Electronic Disruption
- Weapons of Mass Destruction

Terrorists employ a variety of methods to achieve their goals including bombings, hostage taking, sabotage, hijacking, arson, assault, electronic disruption, and weapons of mass destruction. In carrying out their attacks, terrorists can be ruthless, resourceful, intelligent, and patient.

International Terrorism in the Modern World

- **Terrorism is a Global Threat**
  - **Multiple Incidents Occurring Simultaneously at Different Locations**
  - **Threat to Continental United States, International Partners, and U.S. Interests Abroad**
- **Terrorists Employ Conventional and Unconventional Weapons**
  - **Improvised Explosive Devices (IEDs)**
  - **Weapons of Mass Destruction (WMDs)**
  - **Airplanes**
- **Terrorism and globalization**
  - **Decreased costs of communication and travel**
  - **Widespread access to information**
  - **Porous borders**



Terrorism today is no longer limited to large consolidated groups masterminding single attacks. Nor is it limited by territorial boundaries. Terrorism today may involve multiple incidents, coordinated at multiple locations. It may involve suicidal attacks or biological warfare. Terrorists have seized upon the same means and methods that make international business flow or transnational travel so easy – i.e. global communication networks, porous borders, rise of international markets. Today, modern terrorism often consists of global networks with isolated cells masterminding several different, coordinated attacks on civilian targets. The wrath of al-Qaeda and other such organizations is not confined to the government of a nation, it may also target our entire society - our people, our culture, our very way of life.

1. Terrorism is now a global problem. It spans nations and alliances. It is no longer simply an exterior threat; rather, it is a threat that can lay dormant within our own borders if we allow it to.

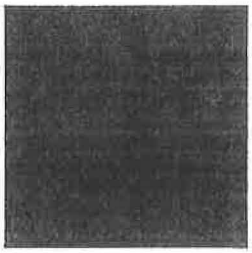
2. Terrorist organizations are complex. They rarely utilize a pyramid chain-of-command, but rather a divided cell organization able to mobilize independently and without warning. These cells can receive funding from a variety of sources and are located around the world.

3. In addition, terrorists have collected a variety of weapons with which to wage their attacks. They use conventional weapons such as guns and car bombs, unconventional weapons such as airplanes and shoe bombs. As you observe in the photograph, terrorist have outfitted an ordinary car with explosives. Terrorists are also interested in adding weapons of mass destruction to their arsenal, using biological, chemical, nuclear and radiological weapons to increase their capacity for violence and destruction.

4. Terrorist have also adapted technology to their own ends. They have seized upon the anonymity of internet addresses, cellular telephones, and cable internet providers. They have used technological knowledge to obtain false identities and produce false identification.

Weapons of Mass Destruction

- Include biological, chemical, nuclear and radiological weapons.
- Small-scale chemical and biological attacks have already occurred; larger scale attacks are possible.


One of the greatest threats the United States faces today is a terrorist attack employing weapons of mass destruction (WMDs). WMDs can be thought of as super-weapons with a domestic destructive capacity that far exceeds that of conventional weapons. WMDs include biological, chemical, nuclear, and radiological weapons. WMDs are characterized by the enormous scale of destruction and devastating residual effects that these weapons can cause. To understand the unique destructive capability of WMDs one need only imagine the damage that would occur if a nuclear device were ever detonated in a major city: hundreds of thousands would be killed with the initial blast, while the fallout would likely kill tens of thousands more—not to mention billions of dollars in property damage and the debilitating fear that would spread throughout society. Potentially even more destructive would be a successful biological attack that released a powerful strain of a deadly virus that spread quickly throughout a population, leaving hundreds of thousands, if not millions, dead in its wake.

The capacity for weapons of mass destruction has existed for a number of years, but has remained under tight control. Their use in warfare has been banned by international treaties. Despite (or because of) the enormous power of these weapons, WMDs are a powerful deterrent for nations because of the principle of deterrence (if you use them against us, we'll use them against you). Deterrence has been effective in keeping the peace between hostile nuclear powers such as the United States and the Soviet Union during the Cold War, and India and Pakistan.

The principle of deterrence breaks down when applied to terrorists who believe their cause is worth their death and the death of many others.

The threat of terrorists using weapons of mass destruction is very real. In fact, some biological and chemical attacks have already occurred. On March 20, 1995, members of Aum Shinrikyo, an apocalyptic Japanese religious cult, simultaneously released the chemical nerve agent Sarin on several subway trains across Tokyo, killing 12 and injuring close to 1500. Additionally, in late 2001 a number of deaths occurred within the United States as anthrax was spread through the postal system. While the impact of these attacks in Tokyo and the United States was relatively limited when considered against the potential destruction these weapons can cause, the threat of a much larger scale attack occurring in the future must not be underestimated. With "loose nukes" still unaccounted for in the former Soviet Union, two state sponsors of terrorism rapidly advancing their nuclear capabilities (North Korea and Iran), and nuclear black markets run by rogue scientists such as Pakistan's A.Q. Khan, the possibility of terrorists getting their hands on these dangerous weapons is all too real.

Since 9/11, public attention has focused primarily on international terrorism. However, domestic terrorism continues to pose a considerable threat to our nation's security. Domestic terrorism is defined according to three characteristics: 1) the nature of the conduct committed; 2) the intent of the actors; and 3) the location of the conduct committed. Generally speaking, domestic terrorism can be defined as violence committed by U.S. nationals within the territorial jurisdiction of the United States intended to intimidate or coerce a civilian population and/or influence the policy of the government through coercion and intimidation. There are many different kinds of domestic terrorist groups across the United States, ranging from animal rights extremists, sovereign citizen groups, and white supremacists. No matter what their individual cause, domestic terrorist groups are ready and willing to use violence against citizens and the government to pursue their social and political objectives.

How do we Identify the enemy?

- Terrorists are elusive enemies difficult to define, target, and eliminate.
- One important strategy the United States has developed is to list known terrorists and terrorist supporters, apply sanctions to the individuals and entities listed, and punish those who engage in prohibited activity with listed individuals, groups, or states.

Because terrorists are more difficult to identify, locate and observe/monitor than a hostile state, the U.S. government relies on a number of different terrorist lists to keep track of individuals and entities that are known to engage in or actively support terrorist acts around the world. This allows us to clearly identify the enemy, isolate them from the rest of society, and use a variety of methods to shut down their violent and unlawful activity, through the use of the rule of law.

Advantages of Terrorist Lists

- Bring legal clarity to our efforts to identify and prosecute members and supporters of terrorist organizations.
- Provide focal point for coordination of Executive agencies' counterterrorist efforts.
- Provide focal point for coordination of international counterterrorist efforts—international alliance against a common enemy.
- Stigmatize listed individuals, groups, and states.

Other countries, including Canada and the United Kingdom, also use the list-based approach in their efforts against terrorism.

Disadvantages of Terrorist Lists

- Lack the flexibility needed to keep up with continually evolving groups.
- Do not effectively deal with ad hoc activities engaged in by terrorist "freelancers" or "lone wolves".

There are also some disadvantages associated with terrorist lists. First, terrorist groups are emerging and evolving more quickly than our bureaucracy can detect and respond. Thus, the most common criticism of the list system is that it is too restrictive and inflexible to cope with an area of foreign policy that requires maximum flexibility. This issue was partially dealt with in the Intelligence Reform and Terrorism Prevention Act of 2004, which greatly eased the requirements for redesignating FTOs every 2 years after their initial designation.

Another drawback to the list system is that it fails to effectively address increasing amounts of "freelance" terrorist activity. Many terrorist cells operating around the world today are essentially independent groups with only loose, ideological affiliation to designated organizations, such as Al Qaeda. While these "terrorist freelancers" may claim to have been acting on behalf of a certain organization, these ties are often very tenuous and may be difficult to prove in court. Thus while lists are useful for disrupting the activities of individuals with clear, demonstrable ties to designated terrorist entities, they do not effectively address the growing number of extremists who act independently.

Foreign Terrorist Organizations

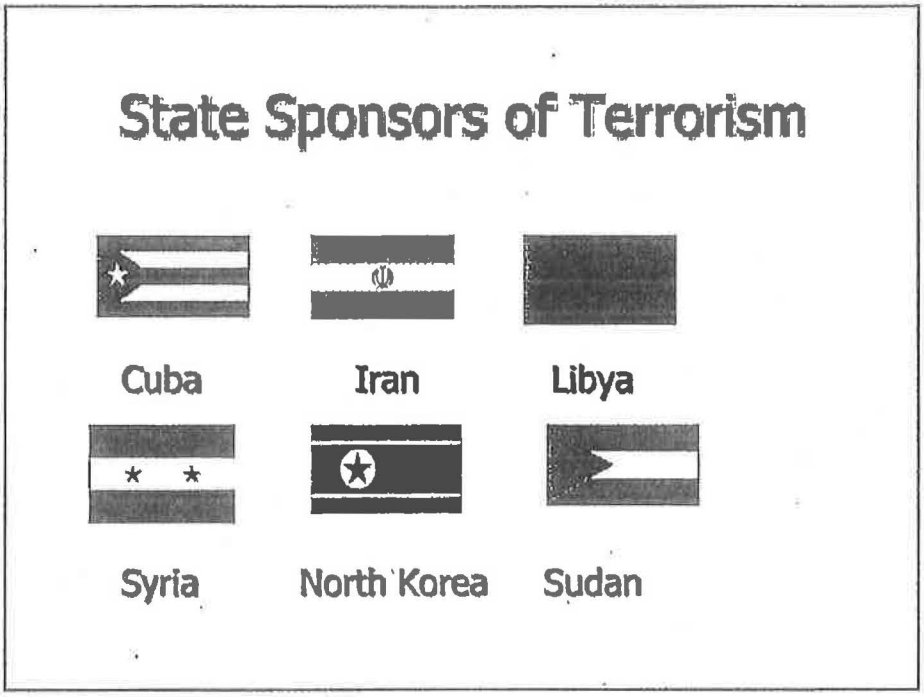
- **"Foreign Terrorist Organization" is defined as:**
- **A foreign organization;**
- **That engages, or has the capability to engage, in terrorist activity;**
- **That threatens the national security of the United States or the security of U.S. Nationals.**

Foreign Terrorist Organizations (FTO) are foreign organizations that are designated by the Secretary of State, in consultation with the Attorney General and the Secretary of the Treasury, in accordance with Section 219 of the Immigration and Nationality Act. Once a group is designated, it is illegal to provide money or other types of support to the group or its members, and members are barred from the U.S. FTO designations play a critical role in our fight against terrorism and are an effective means of curtailing support for terrorist activities and pressuring groups to get out of the terrorism business. The Office of the Coordinator for Counterterrorism in the State Department continually monitors the activities of terrorist groups active around the world to identify potential candidates for designation. The Attorney General has also suggested certain groups for designation. Designation is predicated, not only on actual terrorist attacks that a group has carried out, but also on whether the group has engaged in planning and preparations for possible future acts of terrorism or retains the capability and intent to carry out such acts.

Foreign Terrorist Organizations

- Abu Nidal Organization (ANO)
- Abu Sayyaf Group
- Al-Aqsa Martyrs Brigade
- al-Jihad (Egyptian Islamic Jihad)
- al-Qa'ida
- Ansar al-Islam
- Armed Islamic Group (GIA)
- Asbat al-Ansar
- Aum Shinrikyo
- Basque Fatherland and Liberty (ETA)
- Communist Party of the Philippines/ New People's Army
- Continuity Irish Republican Army (CIRA)
- Gama'a al-Islamiyya (Islamic Group)
- HAMAS (Islamic Resistance Movement)
- Harakat ul-Mujahideen (HUM)
- Hizballah (Party of God)
- Islamic Jihad Group
- Islamic Movement of Uzbekistan (IMU)
- Jaish-e-Mohammed (JEM) (Army of Mohammed)
- Jemaah Islamiya
- al-Jihad (Egyptian Islamic Jihad)
- Kahane Chai (Kach)
- Kongra-Gel (KGK, Fomerly Kurdistan Workers' Party (PKK))
- Lashkar-e Tayyiba (LT) (Army of the Righteous)
- Lashkar I Jhangvi
- Liberation Tigers of Tamil Eelam (LTTE)
- Libyan Islamic Fighting Group (LIFG)
- Moroccan Islamic Combatant Group (GICM)
- Muhahedin-e Khalq Organization (MEK)
- National Liberation Army (ELN)
- Palestine Liberation Front (PLF)
- Palestinian Islamic Jihad (PIJ)
- Popular Front for the Liberation of Palestine (PFLP)
- PFLP- General Command (PFLP-GC)
- Real IRA
- Revolutionary Armed Forces of Colombia (FARC)
- Revolutionary Nuclei (ELA)
- Revolutionary Organization 17 November
- Revolutionary People's Liberation Army/Front (DHKP/C)
- Salafist Group for Call and Combat (GSPC)
- Shining Path (Sendero Luminoso, SL)
- Tanzim Qa'idat al-Jihad fi Bilad al-Rafidayn (QJBR) (al-Qaida in Iraq)
- United Self-Defense Forces of Colombia (AUC)
- http://www.state.gov/s/ct/rls/fs/37191.htm

As of July, 2006, there are 42 groups designated as Foreign Terrorists Organizations.



The U.S. government has a number of other mechanisms to track terrorists and their supporters. One mechanism is the designation of "state-sponsors of terrorism", pursuant to section 6(j) of the Export Administration Act of 1979. Under the terms of the Act, the Secretary of State provides Congress with the list of countries that have "repeatedly provided support for acts of international terrorism." These countries are subject to a range of severe U.S. export controls, especially of dual-use technology and weapons. As of June, 2006, there are six states designated as state-sponsors of terrorism: Cuba, Iran, North Korea, Sudan, Syria, and Libya. Although the intention to remove Libya was recently announced on May 15, 2006, they currently remain on the list.

Other Terrorist Designations

- Specially Designated Terrorists (SDT)
- Specially Designated Global Terrorists (SDGT)
- SDT + SDGT + FTO + State Sponsors of Terrorism = Specially Designated Nationals and Blocked Persons (SDN)
- Terrorist Exclusion List (TEL)

(SDN)http://www.treas.gov/offices/enforcement/ofac/sdn/t11sdn.pdf

Two additional terrorist lists were created pursuant to the International Emergency Economic Powers Act. The "specially designated terrorists" (SDTs) list, created in 1995 to block the assets of individuals and groups that threatened to disrupt the Middle East Peace Process, was later expanded into the Specially Designated Global Terrorists (SDGTs) list following the events of September 11, 2001. These lists are used to block "all property and interests in property" of certain designated terrorists and the individuals and entities supporting them.

In October 2002, the SDT, SDGT, state sponsors, and FTO lists were combined into one comprehensive roster called the "Specially Designated Nationals and Blocked Persons" (SDN) list. This list is maintained by the Office of Foreign Assets Control of the Treasury Department. While the individual lists that make up the SDN list retain their separate identity pursuant to their specific legislation, the SDN list presents in one place all of the terrorist entities that are economically sanctioned by the United States.

Additionally, the "Terrorist Exclusion List" (TEL), created pursuant to Section 411 of the USA PATRIOT Act of 2001, is used to designate terrorist organizations strictly for immigration purposes.

Examples of Terrorist Acts

- **1993 NYC World Trade Tower**
- **1998 U.S. Embassies in Kenya and Tanzania**
- **2000 U.S.S. Cole**
- **2001 NYC World Trade Towers and the Pentagon**
- **2002 Bali resort**
- **2003 Casablanca**
- **2004 Madrid**
- **2005 London**

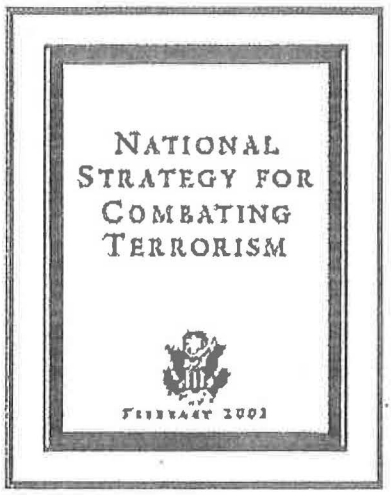
The world has experienced many acts of terrorism in recent times: Most notably for Americans, September 11, 2001. Other significant recent attacks include the destruction of U.S. embassies in Kenya and Tanzania; the attack on the U.S.S. Cole; and the bombing of a Bali resort on October 12, 2002. The attack in Bali alone killed over 200 people from several different nations (Australia, Britain, Indonesia, Germany, Sweden, United States, Denmark, Switzerland, Japan, France, South Korea, Canada, Ecuador, Netherlands, New Zealand, Singapore, South Africa, Taiwan). Terrorists have sought out numerous targets using a variety of violent means with all too much success.

It is our job to stop them.

SECTION II

DOJ Strategy for Combating Terrorism

National Strategy for Combating Terrorism



- Defeat
- Deny
- Diminish
- Defend

The National Strategy for Combating Terrorism, published in February 2003, acknowledges that terrorism is not a new problem, recognizes the changing nature of terrorism, and emphasizes the need for our nation and our allies to put an end to the terrorist groups and individuals who seek to exploit disadvantaged communities and destroy free nations. As noted in the strategy, "States that have sovereign rights also have sovereign responsibilities."

The National Strategy for Combating Terrorism outlines a 4 pronged approach to comprehensively counter terrorist action on all fronts. It is the "defeat," "deny," "diminish," and "defend" strategy – the 4D strategy.

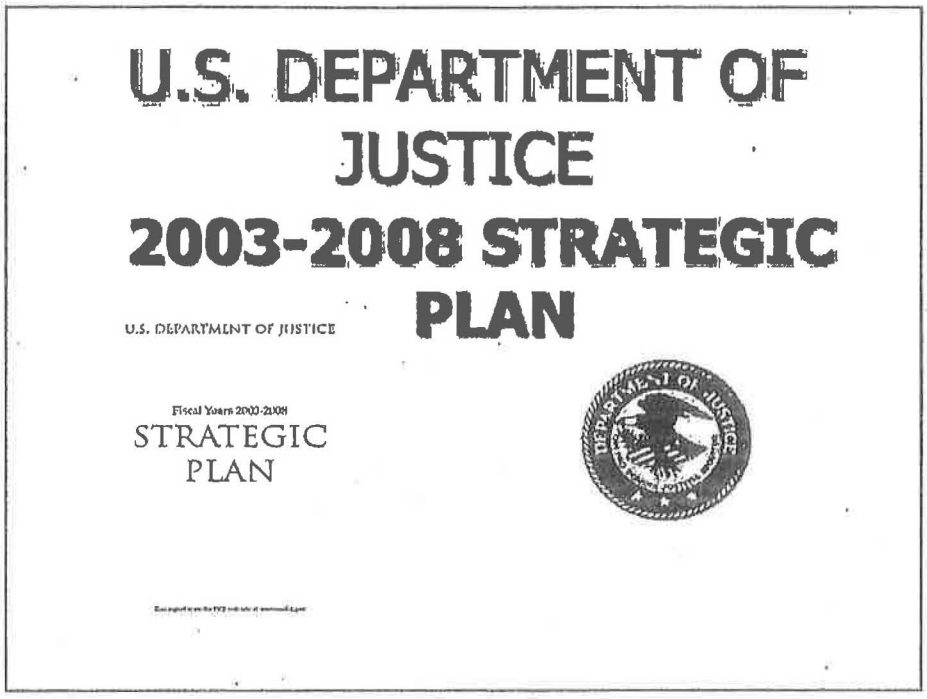
"The United States and its partners will ***defeat*** terrorist organizations of global reach by attacking their sanctuaries; leadership; command, control, and communications; material support; and finances."

"We will ***deny*** further sponsorship, support, and sanctuary to terrorists by ensuring other states accept their responsibilities to take action against these international threats within their sovereign territory."

"We will ***diminish*** the underlying conditions that terrorist seek to exploit by enlisting the international community to focus its efforts and resources on the areas most at risk."

"[W]e will ***defend*** the United States, our citizens, and our interests at home and abroad by both proactively protecting our homeland and extending our defenses to ensure we identify and neutralize the threat as early as possible."

The USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) is an important measure in ensuring that we can meet these objectives and fulfill our responsibilities as a sovereign nation. The Act provides the tools and resources necessary to investigate and prosecute terrorism as well as meet the objectives of the National Strategy for Combating Terrorism. These tools have been enhanced, expanded, and reinforced by the Intelligence Reform and Terrorism Prevention Act of 2004 (IRPTA) and the USA PATRIOT Act Improvement and Reauthorization Act (IRA).

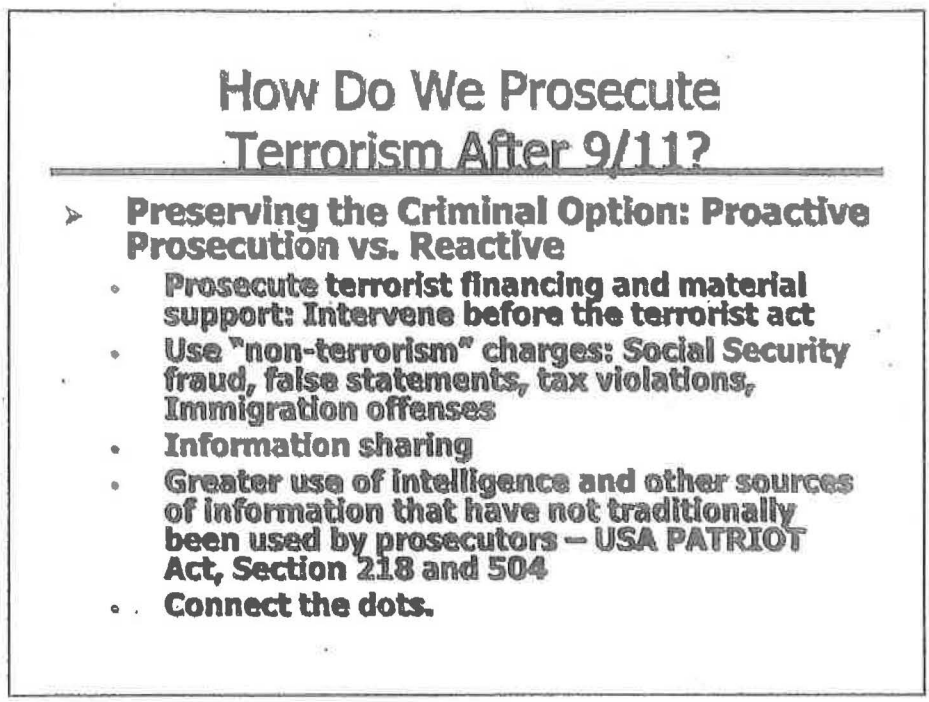


The number one strategic goal in the Department of Justice's Strategic Plan for 2003-2008 is "the protection of America against the threat of Terrorism and National Security." The stated objectives to achieve that goal are to "prevent, disrupt, and defeat terrorist operations before they occur"; "develop and implement the full range of resources available to investigate terrorists incidents, bringing their perpetrators to justice"; and to "vigorously prosecute those who have committed, or intend to commit, terrorists acts in the United States."

DOJ Counterterrorism Policy
Post-9/11

- **Traditionally, terrorism has been investigated and prosecuted reactively—after a terrorist event occurs.**
- **Following 9/11, the Justice Department's policy has focused on PREVENTION.**
- **We will use all of our laws to disrupt, dismantle, incapacitate and prosecute terrorists.**

Post 9/11, DOJ Counterterrorism policy has changed significantly. Instead of prosecuting reactively – after a terrorist event occurs, the goal is to prevent and disrupt. The DOJ goal is to use all of our laws to first and foremost prevent future terrorist attacks and to disrupt, dismantle, incapacitate and prosecute terrorists.

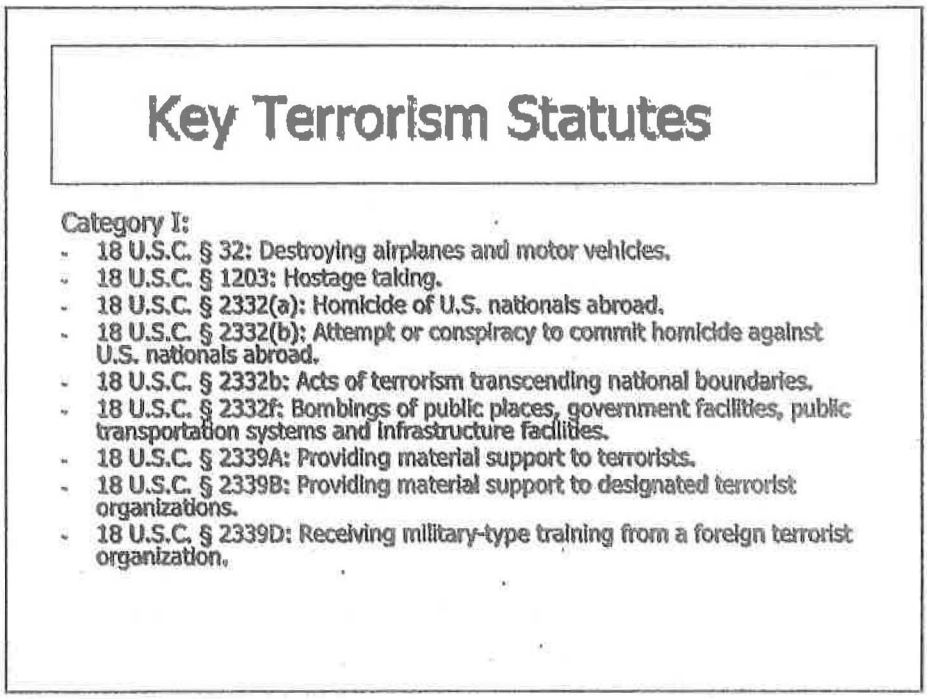


The new focus on prevention requires law enforcement agents and prosecutors to change their previous way of thinking about cases. The current approach recognizes the importance of constant information-sharing; a focus on events earlier in the sequence of events by analyzing methods of terrorist financing and material support; prosecution for any federal offense that might disrupt a terrorist act; and working closely with local JTTFs and Main Justice to coordinate investigations and to both "increase the number of dots" and then connect them using a variety of means, including link analysis—association with people, places or events—and pattern analysis—tracking methods and means characteristic of terrorists.

Legal Authorities and Guidelines

- National Security Presidential Directive (NSPD)
- Homeland Security Presidential Directive (HSPD)
- National Security Directives (NSD)
- Attorney General Guidelines
- National Security Guidelines
- Guidance Concerning Terrorism Matters

A number of different legal authorities and guidelines exist in the national security arena. Many of these are classified, and are thus restricted to those with appropriate clearance and a need-to-know basis.



There are 26 Category I international terrorism statutes. Category I statutes are the criminal statutes that most directly apply to terrorist offenses. Some of the most important of these statutes are listed above.

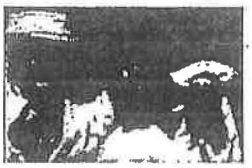
Other Useful Statutes

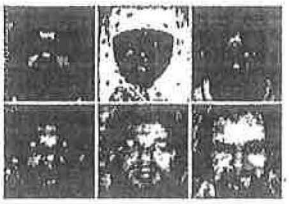
- 18 U.S.C. § 842: Explosives offenses.
- 18 U.S.C. § 1362: Damaging government property and communication lines.
- 18 U.S.C. § 1960: Money laundering.
- 18 U.S.C. § 1001: False statements.
- 18 U.S.C. § 1425: Citizenship and naturalization fraud.
- 18 U.S.C. § 876: Mailing threatening communications in interstate or foreign commerce.
- 18 U.S.C. § 922: Firearms offenses.
- 18 U.S.C. § 1542: Passport/visa fraud.

Outside of the Category I international terrorism statutes, there are many other statutes that, while not specifically tailored for terrorism prosecutions, may be applied to terrorism prosecutions. Some of the most important of these statutes are listed above.

Significant Criminal Terrorism Prosecutions

- John Walker Lindh
- Charlotte Hizballah
- Lackawanna Cell
- Portland Cell
- Virginia Jihad Network
- Enaam Arnaout
- Earnest James Ujaama
- Iyman Faris
- Richard Reid
- Mohammed Junaid Babar





The war on terrorism continues, but through effective investigations and prosecutions, we have achieved some significant results. Examples include:

John Walker Lindh (Eastern District of Virginia) – Lindh pleaded guilty in July 2002 to one count of supplying services to the Taliban and a charge that he carried weapons while fighting on the Taliban's front lines in Afghanistan against the Northern Alliance. Lindh was sentenced to 20 years in prison.

Charlotte Hizballah: (Western District of North Carolina) – Mohamad Hammoud and several co-defendants were charged with RICO and material support to terrorism statutes for their involvement in a Charlotte-based Hizballah cell that engaged in a cigarette tax evasion scheme and in military procurement ordered by Hizballah leaders in Lebanon. Brothers Mohamad and Chawki Hammoud were convicted in June 2002 and sentenced in February 2003. The Fourth Circuit has since remanded the case for re-sentencing. Hassan Makki, who pled guilty to RICO conspiracy and providing material support to Hizballah in the Eastern District of Michigan, has been sentenced to 57 months in prison.

Lackawanna Cell: (Western District of New York) – Six defendants from the Lackawanna, New York area (Shafal Mosed, Yahya Goba, Sahim Alwan, Mukhtar Al-Bakri, Yasein Taher, and Elbaneh Jaber) pleaded guilty to charges of providing material support to al Qaeda, based on their attendance at an al Qaeda terrorist training camp. The defendants were sentenced to terms ranging from seven years to ten years in prison.

Portland Cell: (District of Oregon) – The defendants in the so-called "Portland Cell" case (Maher "Michael" Hawash, October Martinique Lewis, Habis Abdullah Al-Saoub, Patrice Lamumba Ford, Ahmed Ibrahim Bilal, Muhammad Ibrahim Bilal, and Jeffrey Leon Battle) pleaded guilty to criminal charges ranging from laundering money to conspiracy to supply goods to the Taliban, to seditious conspiracy. Ford and Battle were each sentenced to 18 years in prison. The charges resulted from an investigation into the defendants' training for preparation to fight violent jihad in Afghanistan.

Virginia Jihad Network: (Eastern District of Virginia) – In the Virginia Jihad case, Masound Ahmad Khan was convicted in March 2004 of eight charges including conspiracy to levy war against the United States; providing support to the Taliban and conspiracy to provide support to Lashkar-e-Taiba (LET); and gun violations. He was later sentenced to life in prison. Hammad Abdur-Raheem was convicted on three charges of providing material support to LET, firearms and conspiracy charges, and later sentenced to 52 months in prison on each count. Seifullah Chapman was convicted on five counts, including conspiracy to provide material to LET and weapons charges, and later sentenced to 780 months in prison. Also, six defendants (Aatique Mohammed, Donald Thomas Surratt, Khwaja Mahmood Hasan, Yong Ki Kwon, Randall Todd Royer, Ibrahim Ahmed Al-Hamdi) pleaded guilty to various charges, including conspiracy to commit an offense against the United States and weapons violations, and were sentenced to terms ranging from 46 months to 20 years in prison.

Significant Criminal Terrorism Prosecutions 2005

- Zacarias Moussaoui
- Eric Robert Rudolph
- Ali Al-Timimi
- Hemant Lakhani
- Infocom
- Al-Moayad
- Help the Needy
- Sattar/Stewart

Zacarias Moussaoui: (Eastern District of Virginia) – In April 2005, Zacarias Moussaoui pleaded guilty to six charges against him related to his participation in the September 11th conspiracy. In May 2006, Moussaoui was sentenced to life in prison.

Eric Robert Rudolph: (Northern District of Alabama and the Northern District of Georgia) – In April 2005, Eric Rudolph pleaded guilty to the fatal bombing at Centennial Olympic Park in 1996; the bombing of a family planning clinic in 1997; the bombing of a midtown Atlanta nightclub, the Otherside Lounge, in 1997; and the fatal bombing of a Birmingham family planning clinic in 1998. Rudolph received multiple sentences of life in prison, as well as other lengthy prison sentences, as a result of his plea.

Ali Al-Timimi: (Eastern District of Virginia) – Al-Timimi was convicted in April 2005 on all 10 charges brought against him in connection with the "Virginia Jihad" case. Al-Timimi, a spiritual leader at a mosque in Northern Virginia, encouraged other individuals at a meeting to go to Pakistan to receive military training from Lashkar-e-Taibi, a designated foreign terrorist organization, in order to fight U.S. troops in Afghanistan. Al-Timimi was sentenced to life in prison.

Hemant Lakhani (District of New Jersey) – British national Hemant Lakhani was convicted by a federal jury on charges of attempting to sell shoulder-fired missiles to what he thought was a terrorist group intent on shooting down U.S. airliners. Lakhani was sentenced to 47 years in prison.

Infocom:(Northern District of Texas) – In April 2005, a federal jury convicted Basman, Bayan and Ghassan Elashi, and the Infocom Corporation, on charges of conspiracy to deal in the property of a specially designated terrorist and money laundering. The activities were related to Infocom, an Internet Service provider believed to be a front for Hamas. Hazim and Ihsan Elashi were also convicted in the same case and were sentenced to 66 months and 72 months in prison, respectively.

Al-Moayad: (Eastern District of New York) – In March 2005, a federal jury convicted Mohammad Ali Hasan Al-Moayad, a Yemeni cleric, and Mohammed Moshen Yahya Zayed on charges of providing and conspiring to provide material support and resources to al Qaeda and Hamas. Al-Moayad was sentenced to 75 years in prison; Zayed was sentenced to 45 years in prison.

Help the Needy: (Northern District of New York) – Seven defendants, including the lead defendant, Dr. Rafil Dhafir, and a purported charitable organization were charged with a variety of crimes based on Dhafir's creation and operation of the U.S branch of the charity, known as "Help the Needy." Dhafir and Help the Needy defrauded donors and the Internal Revenue Service in soliciting donations and illegally laundering millions of dollars by transferring funds from the U.S. to Iraq, in violation of U.S. economic sanctions and money laundering statutes. Dhafir was also charged with a number of additional offenses. In February 2005, a jury returned a guilty verdict on 59 of the 60 counts against Dhafir. He was sentenced in October of that year to 264 months in prison. Five of the individual defendants pleaded guilty, cooperated, and testified at Dhafir's trial, including the Executive Director of Help the Needy, Dhafir's accountant, and Dhafir's wife. One individual defendant remains a fugitive and is believed to be in Jordan. The Help the Needy Endowment organization was severed from the Dhafir trial and has since been placed in receivership by the Attorney General of the State of New York, thereby obviating trial and forfeiture proceedings.

Sattar/Stewart: (Southern District of New York) – In February 2005, a federal jury in Manhattan convicted attorney

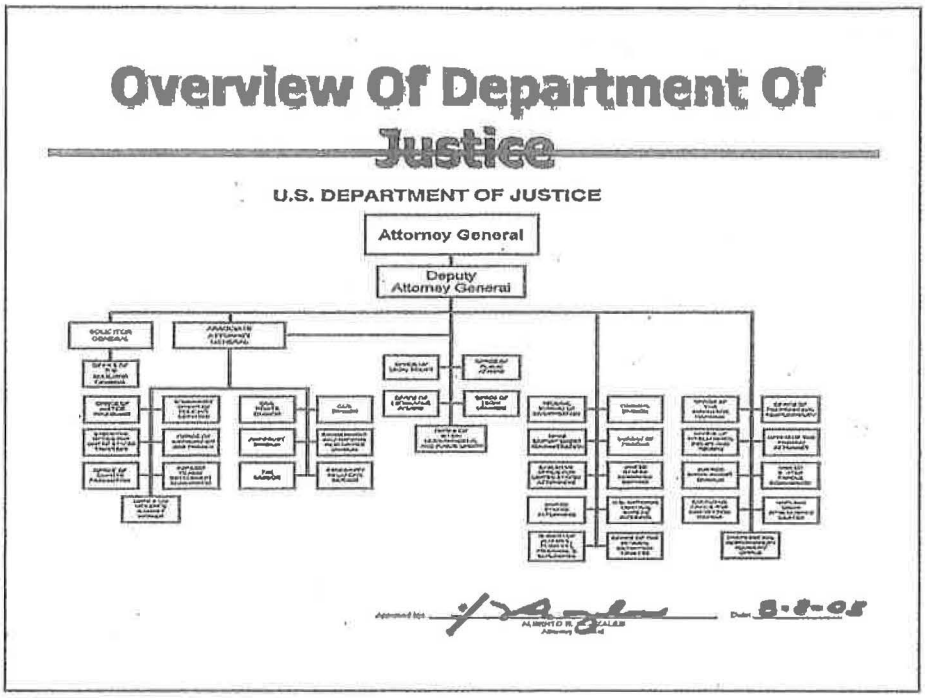
Section III

Organization

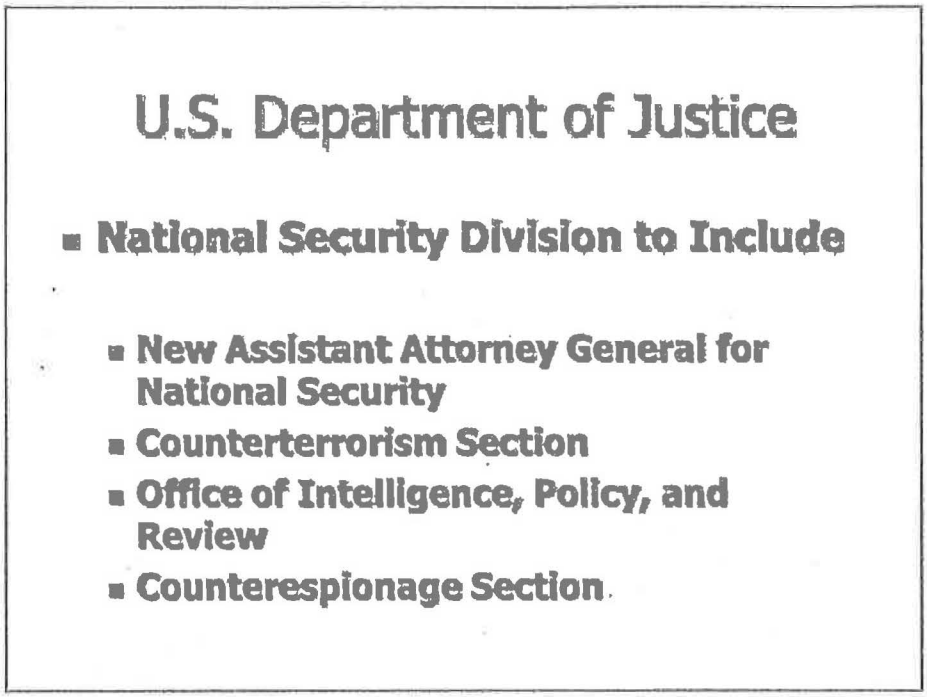
ORGANIZATION

- **What is the Structure and Organization of National Security at DOJ?**
- **What Other National Security Programs Exist?**
- **What Interagency Organizations Exist?**

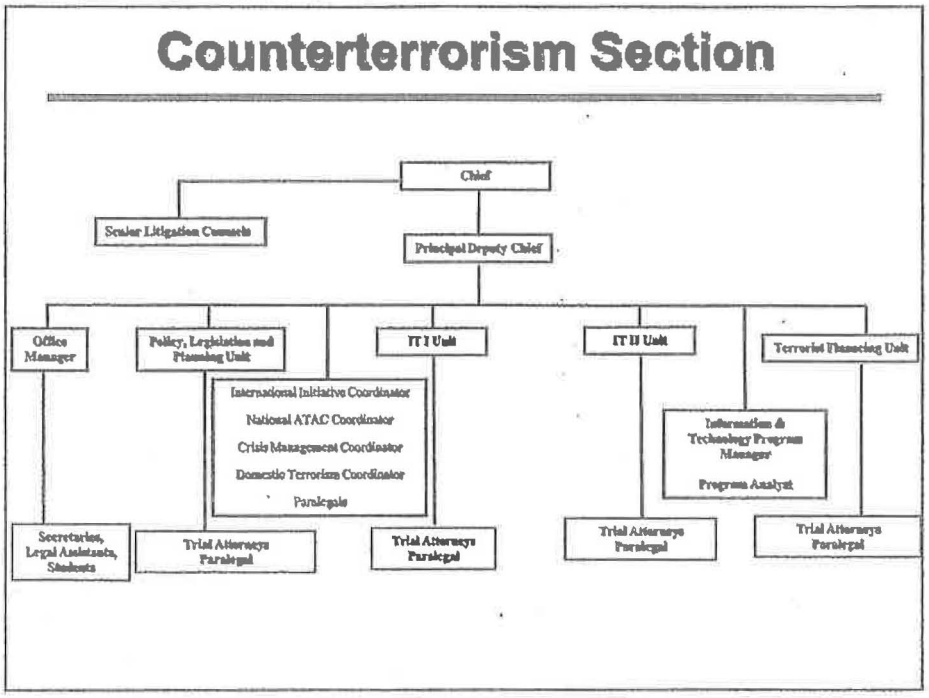
In order to understand how the war against terrorism is implemented, it is helpful to recognize what components support the national security mission within the Department. The next part of this presentation will provide an overview of the structure and organization of National Security at the Department.



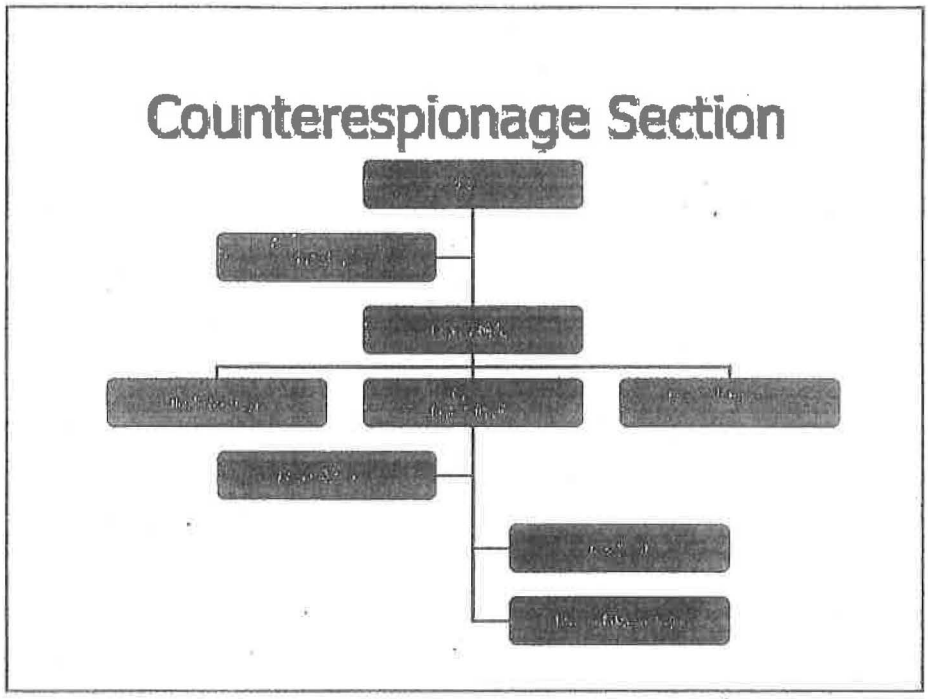
This slide shows the current structure of the Department of Justice. As you can see, the leadership of the Department includes the Attorney General, Deputy Attorney General, Associate Attorney General, Solicitor General, and various heads of Boards, Divisions, and major component agencies such as the Director of the FBI, the Assistant Attorney General of the Criminal Division, and the Commissioner of the Drug Enforcement Agency. The primary Department components involved in national security are the Office of Intelligence Policy and Review, and the Counterterrorism Section and the Counterespionage Section which are both currently located in the Criminal Division, but who will soon be moving to a new National Security Division. The FBI is the primary investigative component for national security matters. Other Department components such as the Office of Legal Counsel and the Office of Legal Policy, are involved in policy, legal advice and interpretation, and legislative aspects of National Security. The mission of the Office of Legal Policy is to plan, develop and coordinate the implementation of major legal policy initiatives of high priority to the Department and to the Administration. OLP functions as a focal point for the development and coordination of Departmental policy. The Office of Legal Counsel assists the Attorney General in his function as legal advisor to the President and all the executive branch agencies. The Office drafts legal opinions of the Attorney General and also provides its own written opinions and oral advice in response to requests from the Counsel to the President, the various agencies of the executive branch, and offices within the Department. The Executive Office for United States Attorneys provides administrative services to the 94 United States Attorneys' Offices



The USA PATRIOT Improvement and Reauthorization Act (IRA) of 2005 created the new National Security Division at the Justice Department consistent with the recommendations made by the WMD Commission. It will place all three core national security components of DOJ – the Counterterrorism Section, the Counterespionage Section, and the Office of Intelligence Policy and Review – under the control of a new Assistant Attorney General. The new AAG, in turn, will serve as the Department of Justice's primary liaison to the Director of National Intelligence (DNI).

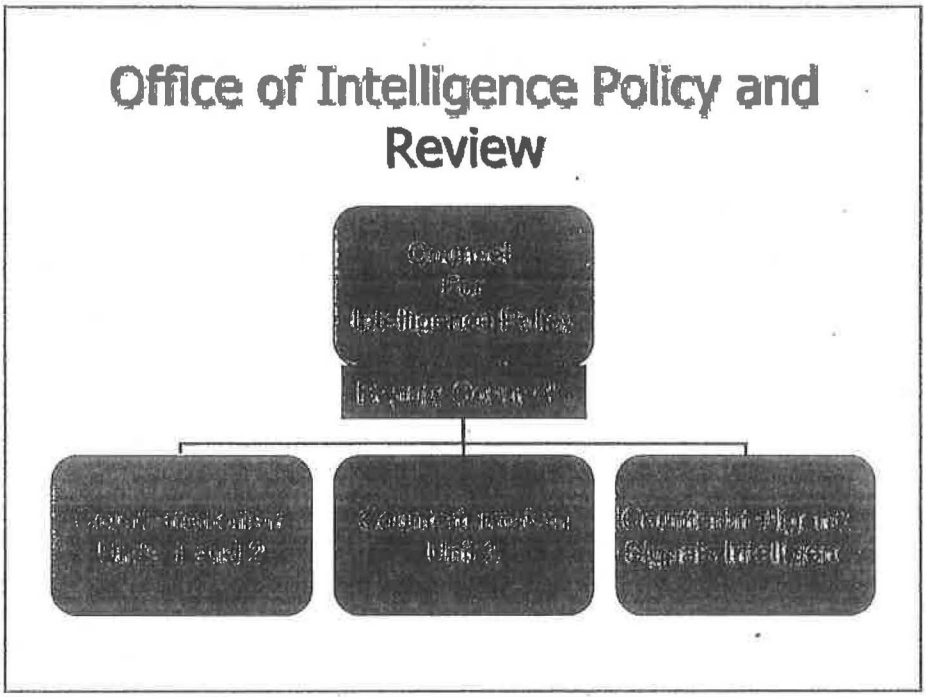


The Counterterrorism Section (CTS) is responsible for coordination of terrorism-related prosecutions and matters throughout the U.S. It works closely with the counterterrorism prosecutors in the United States Attorneys' Offices to assist and provide expertise on terrorism prosecutions. CTS also drafts legislation, proposes and implements policy initiatives and acts as liaison to intelligence agencies and foreign partners on terrorism-related matters.

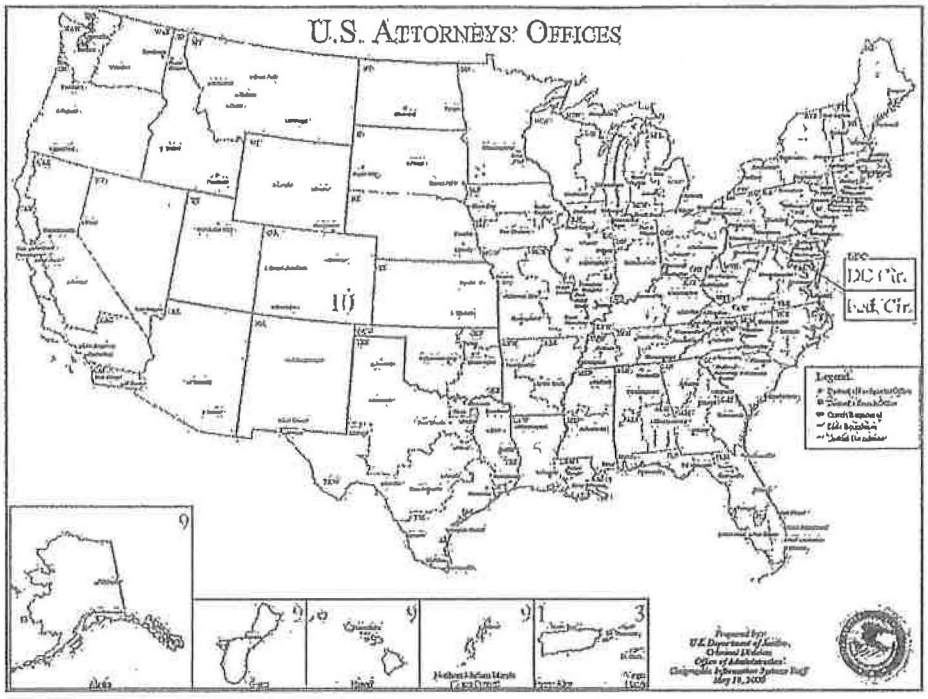


The Counterespionage Section (CES) supervises the investigation and prosecution of non-terrorism cases affecting national security, foreign relations, and the export of military and strategic commodities and technology.

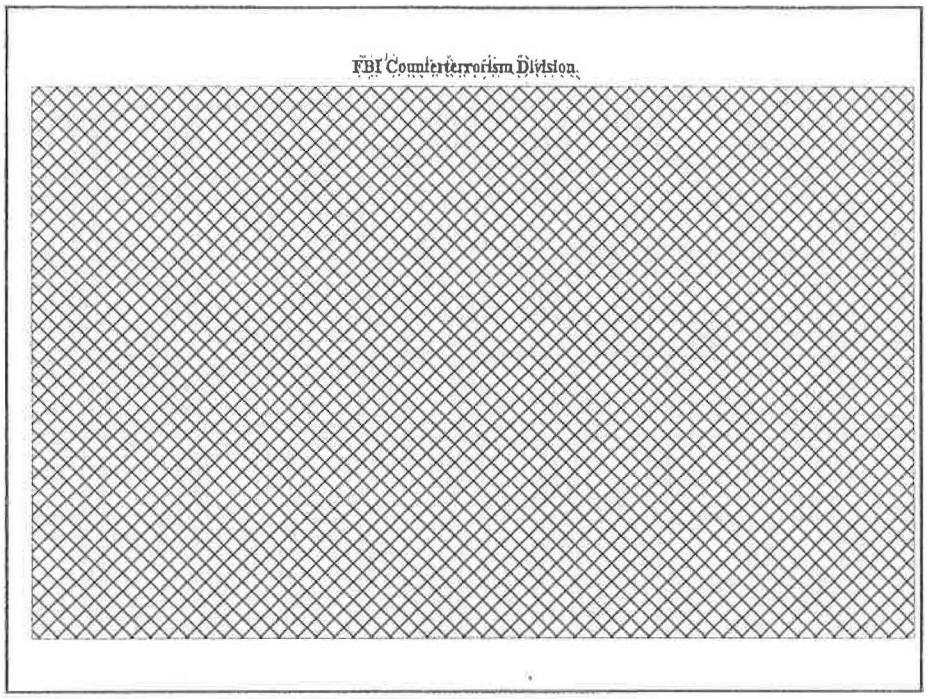
CES has executive responsibility for authorizing the prosecution of cases under criminal statutes relating to espionage, sabotage, neutrality, and atomic energy. CES provides legal advice to United States Attorneys' Offices and investigative agencies on all matters within its area of responsibility, which include 88 federal statutes affecting national security. It also coordinates non-terrorism criminal cases involving the application of the Classified Information Procedures Act.



The Office of Intelligence Policy and Review prepares and files all applications for electronic surveillance and physical search under the Foreign Intelligence Surveillance Act of 1978, assists Government agencies by providing legal advice on matters of national security law and policy, and represents the Department of Justice on a variety of interagency committees such as the National Counterintelligence Policy Board.

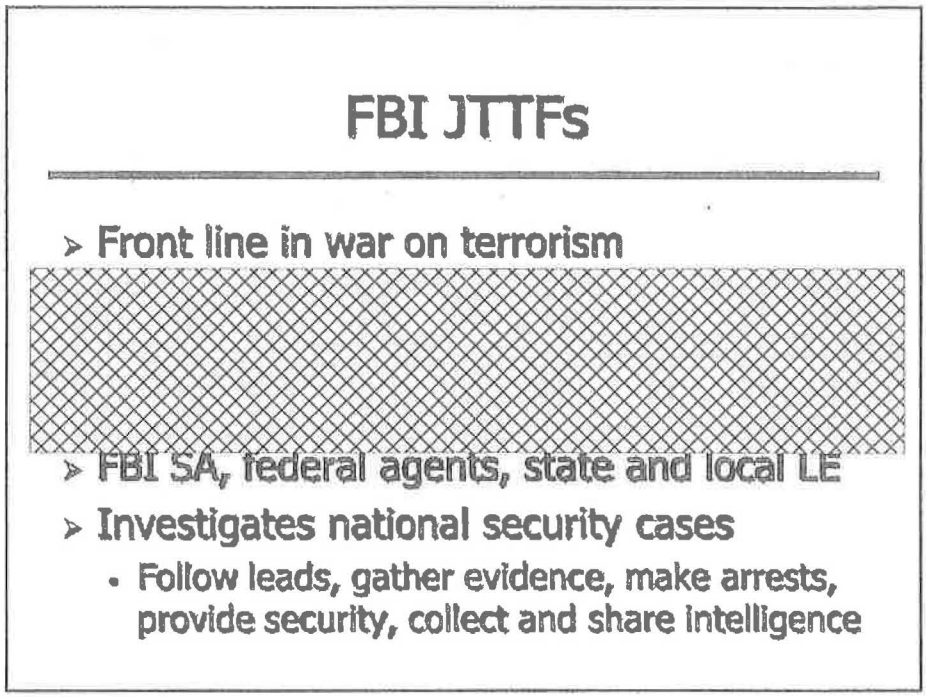


There are 94 United States Attorney's Offices throughout the United States. Each is headed by a United States Attorney who is appointed by the President and confirmed by the Senate. The United States Attorneys' Offices are staffed by Assistant United States Attorneys (federal prosecutors) who serve as the nation's front-line litigators of federal criminal cases and civil matters involving the United States.



b7E per FBI

This is the current organizational structure of the FBI's Counterterrorism Division. The FBI's Counterterrorism Division is undergoing a reorganization and thus this current layout is subject to change.



b7E per FBI

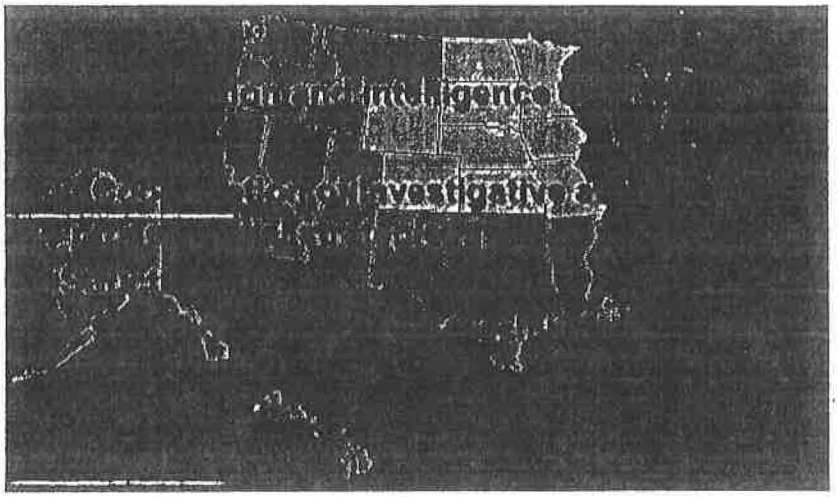
The FBI's Joint Terrorism Task Forces (JTTF) have primary operational responsibility for terrorism investigations. In response to the terrorists acts of September 11, 2001, the FBI expanded the number of JTTFs to the current number of 101. The JTTFs mission is to detect and investigate terrorists and terrorist groups and prevent them from carrying out terrorist acts directed against the United States. Membership in the JTTF is limited to law enforcement, intelligence, and military personnel with security clearances.

Anti-Terrorism Advisory Councils (ATACs)

- Councils chaired by the U.S. Attorney
- Members include federal, state and local LE
- A LE forum tailored to each judicial district
- Focus on terrorism prevention, information-sharing, and training.
- Private sector participation

The Anti-Terrorism Advisory Councils (ATACs), led by an experienced Anti-Terrorism prosecutor called the ATAC Coordinator, exists in every United States Attorneys' Office and serves as a standing organizational structure to address terrorism matters in each district. While working closely with the JTTFs, the ATACs serve as a conduit of information about suspected terrorists among the federal and local law enforcement agencies, focusing on timely information-sharing and training. The ATACs are part of a national network that coordinates the dissemination of information and the development of investigative and prosecutive strategy throughout the country. The ATACs are open to a broad range of participants and do not require security clearances.

Anti-Terrorism Advisory Councils (ATACs)



The 93 ATACs (there are 94 United States Attorneys' Offices, but one ATAC Coordinator serves both the District of Guam and the Northern Mariana Islands) are grouped into 6 ATAC regions and are coordinated by six Regional Coordinators and a National Coordinator in the Counterterrorism Section of the Department. The Regional Coordinators work closely with the ATAC Coordinators in the United States Attorneys' Offices to coordinate investigations and prosecutions, support training, and ensure that the ATAC Coordinators receive pertinent information about National and Department policies and legislation. Intelligence Research Specialist in the United States Attorneys' Offices facilitate the information sharing process and collaborate with other intelligence specialists (state, local, federal) within each District.

Section IV

National Security Tools and Techniques

NATIONAL SECURITY TOOLS AND TECHNIQUES

- **WHAT TOOLS DO WE USE IN NATIONAL SECURITY INVESTIGATIONS?**
- **WHAT TOOLS DID THE USA PATRIOT ACT AND SUBSEQUENT LEGISLATION GIVE US?**
- **HOW DO INTELLIGENCE INVESTIGATIONS DIFFER FROM CRIMINAL PROSECUTIONS?**

The next part of this presentation will focus on the tools that are used in national security investigations, including the new tools provided through the USA PATRIOT Act and the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). We will also discuss how intelligence investigations differ from criminal prosecutions, and some of the factors considered in how these cases are pursued.

INFORMATION COLLECTION TOOLS

- FISA
- TITLE III INTERCEPT
- CONSENSUAL RECORDING
- TITLE 18 PEN REGISTER
- TRAP AND TRACE ORDER
- RULE 41 SEARCH WARRANT
- NATIONAL SEARCH WARRANT
- NATIONAL SECURITY LETTER
- INTERVIEW
- GRAND JURY SUBPOENA
- MAIL COVER
- TAX INFORMATION

These are investigative tools commonly used in national security investigations.

The Patriot Act is…

-Information sharing (203-GJ; 218-FISA)

-Stronger criminal laws to combat terrorism

-Material Support (811—conspiracy/attempt)

-Sentencing (810—increases max penalties)

-Extension of tools used in other areas of criminal law (delayed notice warrant 213)

-Immigration and border protection provisions (Title IV)

-Support for terrorism victims (Title VI)

-New technologies and threats

-(219-Single jurisdiction search warrants)

-(220 Nationwide search warrants)

-Increased government personnel and resources

-(205-FBI Translators)

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)

- Amends FISA to redefine "agent of a foreign power" to include non-U.S. persons who engage in, or prepare for acts of international terrorism.
- Clarifies and expands the material support statutes.
- Permits sharing of grand jury information with foreign governments.
- Criminalizes many hoaxes concerning terrorist acts.
- Creates new offenses relating to missile systems designed to destroy aircraft.
- Facilitates pretrial detention for numerous serious offenses.

Aside from restructuring the intelligence community, the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 also strengthened existing legal tools and created important new ones to enhance our investigative and prosecutorial counterterrorism efforts.

USA PATRIOT Act 2001 Renewal

2 new Public Laws	
Public Law 109-177	**Public Law 109-178**
USA PATRIOT Improvement and Reauthorization Act of 2005. "USA PATRIOT IRA"	USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006.

Changes Made by the PATRIOT Act Renewal

- 1 - Sunset Provisions.
- 2 - Changes in FISA tools.
- 3 - Changes in National Security Letters.
- 4 - Changes at the U.S. Dept. of Justice.
- 5 - Changes Law Enforcement tools.
- 6 – Data-Mining

-The USA PATRIOT Act IRA made 14 of the 16 sunset provisions permanent with the exception of a 4 year sunset provision for USA PATRIOT Act 2001 Section 206 FISA Roving surveillance and USA PATRIOT Act 2001 Section 215 FISA Business Records.

-The USA PATRIOT Act IRA also reflected changes in FISA tools to include changes in FISA Durations; FISA Roving Surveillance; FISA Business Records;

FISA Pen Register/Trap and Trace; and FISA Oversight.

-The additional reauthorizing amendments also included changes in National Security Letters, including changes to

- Confidentiality – nondisclosure provision;
- Recipient challenge/Judicial review;
- Enforcement of NSLs;
- Violation of nondisclosure provision; and
- Changes to Congressional reporting.

-The USA PATRIOT Act IRA included a reorganization of the Department of Justice consistent with the Weapons of Mass Destruction Commission recommendation. This reorganization places all three core national security components of DOJ – the Counterterrorism Section, the Counterespionage Section, and the Office of Intelligence Policy and Review – under the control of a new Assistant Attorney General.

The new AAG will be DOJ's primary liaison to the Director of National Intelligence.

Protecting Civil Liberties

- The PATRIOT Act and subsequent PATRIOT Act Reauthorization legislation ALL include the following:
- - congressional and judicial oversight.
  - principles of privacy established by our constitution.
  - legal standards such as probable cause and court orders.
  - prohibition of investigations of U.S. nationals based solely on first amendment activities.

As we continue the fight against terrorism, it is crucial that we faithfully uphold the Constitution. While Congress has empowered the government with a number of important new tools to help us effectively confront the terrorist threat, Congress has also created a number of safeguards to ensure that the civil liberties of the American people are protected.

National Security Investigation

- LAW ENFORCEMENT: THE BIG QUESTION
- DO WE CONTINUE TO INVESTIGATE AND/OR GATHER INTELLIGENCE OR DO WE ARREST AND PROSECUTE?
- WEIGHING THE EQUITIES OF BOTH SIDES

Traditionally, terrorism has been prosecuted reactively—after a terrorist event occurs.

Now, prevention may include prosecution, but the endgame may not. Whether prosecution will be the ultimate goal will depend not only on the goals and equities of all agencies involved, but ultimately on what will best protect the United States.

Making the Criminal Case

- What is your goal for the investigation?
  - What is your disruption strategy to achieve that goal?
    - What do you need to prove your criminal case?
      - How do you obtain the proper evidence?

These are some of the questions that law enforcement agents and prosecutors should consider when determining how a case should proceed. In the post 9/11 world, success is no longer measured by the number of convictions. Protecting national security must involve a broader focus that emphasizes constant communication, coordination, and decision-making between the intelligence and law enforcement communities.

Section V

Handling National Security Information

What is Classified Information?

Information concerning the national defense or foreign relations of the United States whose unauthorized disclosure could cause damage to the United States.

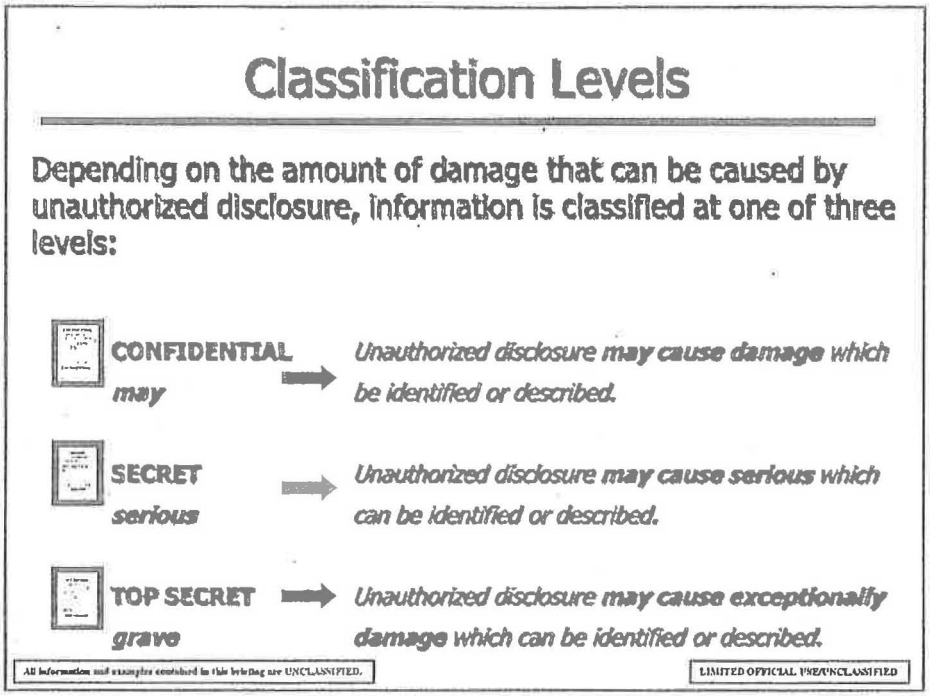
Examples of the types of information that can be classified include:

- **Military plans or weapons systems.**
- **Information provided in confidence by a foreign government or intelligence service.**
- **Information that would damage the foreign relations of the United States.**
- **Information that would reveal the identity of an intelligence source.**
- **Information that would reveal a method of intelligence collection.**

LIMITED OFFICIAL USE/UNCLASSIFIED

The basis for classifying information is **Executive Order 12958 as amended,** which deals with National Security Information (NSI). NSI is "**any information concerning the national defense or foreign relations of the United States whose unauthorized disclosure could cause damage to the United States.**" As you can see, that's a fairly broad definition that could be subject to interpretation. To remove any doubt, the United States classifies information at various levels of sensitivity to ensure adequate protection.

Listed here are several examples of information that can be classified. To ensure that nothing is left to chance, **classification labels are used to clearly identify classified material.**



There are three categories of classification – CONFIDENTIAL, SECRET, and TOP SECRET. Information is classified according to the amount of damage that can be caused by its unauthorized disclosure.

CONFIDENTIAL information corresponds to blue labels and cover sheets.
SECRET information corresponds to red labels and cover sheets, and
TOP SECRET information corresponds to orange labels and cover sheets.

And as you can see here, unauthorized disclosure of CONFIDENTIAL information **may cause damage** to the United States, unauthorized disclosure of SECRET information **may cause serious damage** to the United States, and unauthorized disclosure of TOP SECRET information **may cause exceptionally grave damage** to the United States.

The degree of damage is initially determined by the original classification authority that classified the information.

Why Protect Classified Information?

Disclosure of classified information to persons not authorized to receive it can harm the national security:

- By revealing the ***identity of informants.***
- By compromising technical ***collection methods.***

This risk is present even where the information seems on its face to be innocuous or harmless.

Whatever the case, if the information is classified, it is your responsibility to protect it.

LIMITED OFFICIAL USE/UNCLASSIFIED

So why do we protect classified information in the first place? First and foremost, unauthorized disclosure can be detrimental to our national security.

In addition, unauthorized disclosure can reveal the identity of informants and/or agents. Unauthorized disclosure can also reveal collection methods, processes and sources.

The bottom line is that, **if the information is classified, it is your responsibility to protect it.**

Safeguarding Classified Information

- **Classified information must never be disclosed to persons who do not have appropriate security clearances and "NEED-TO-KNOW."**
- **Classified information can never be discussed, even in vague or indistinct terms, over an unsecure telephone.**
- **Classified information may never be faxed over an unsecure phone/fax.**
- **Computers used for word-processing of classified information must be authorized for such processing (for example, the JCON-S system).**
- **Never e-mail classified information over an unclassified**

The protection of classified information is based on common sense.

"Need to know" seems to be a nebulous concept for many. The rule of thumb is that if you need a piece of information to either **do your job** or to **make a decision**, you probably have a need to know. As you know, technology is rapidly advancing all the time. With those advances come new exploits and vulnerabilities.

Therefore, never discuss classified information over an unsecured phone line and that includes cell phones. Never fax classified information on an unsecured line. And do not process classified information on computers that have not been specifically designed and/or accredited for that level of classification.

Safeguarding Classified Information

- **Never process classified information on a computer connected to the Internet.**
- **All classified information, including working papers, must be properly secured in an appropriate security container when not in use.**
- **Classified information may never be taken home, except with the specific written authorization of the Department Security Officer.**
- **Classified information cannot be sent through the Department's inter-office mail system.**
- **Top Secret material can only be hand delivered by a Top Secret cleared person or courier.**

LIMITED OFFICIAL USE/UNCLASSIFIED

Never process classified information on the computer connected to the Internet.

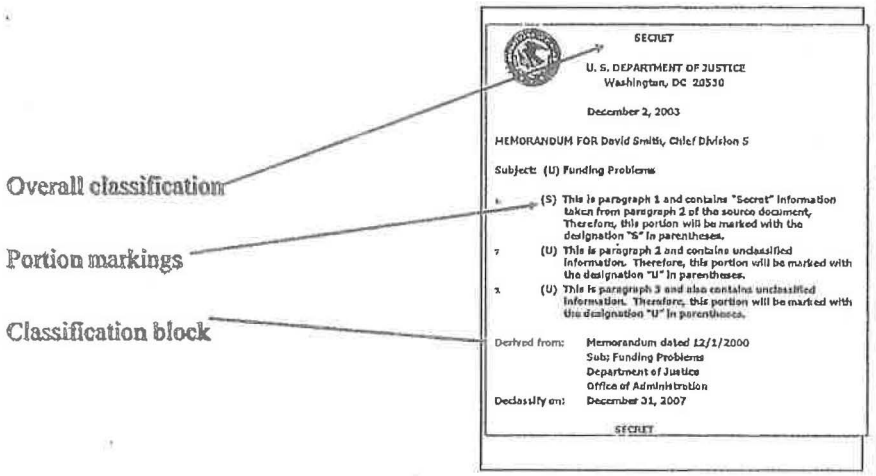
Secure classified information when it is not in use.

You cannot take classified information home unless you have been specifically authorized to do so and have the appropriate secure facilities at that location.

And do not send classified information through interoffice mail.

GET A FULL SECURITY BRIEFING BEFORE HANDLING CLASSIFIED INFORMATION!!!

Marking Classified Information



Overall Marking Guidelines - The highest level of classified information contained in a document shall appear in a way that will distinguish it clearly from the informational text.

Conspicuously place the overall classification at the top and bottom of the outside of the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any).

Each interior page of a classified document shall be marked at the top and bottom either with the highest level of classification of information contained on that page, including the designation "Unclassified" when it is applicable, or with the highest overall classification of the document.

Portion Marking Guidelines Each portion of a document, ordinarily a paragraph, but including subjects, titles, graphics and the like, shall be marked to indicate its classification level by placing a parenthetical symbol immediately preceding or following the portion to which it applies. To indicate the appropriate classification level, the symbols"(TS)" for Top Secret, "(S)" for Secret, "(C)" for Confidential, and "(U)" for Unclassified shall be used.

Original Classification Information - On the face of each originally classified document, including electronic media, the classifier shall apply a "Classified By" line, a "Reason" for the classification and specific "Declassify On" information.

Classification Authority:

Original Classifier. The name or personal identifier, and position title of the original classifier shall appear on the "Classified By" line.

Agency and office of origin. If not otherwise evident, the agency and office of origin shall be identified and placed below the name on the "Classified By" line.

Reason for Classification:

The original classifier shall identify the reason(s) for the decision to classify. The classifier shall include, at a minimum, a brief reference to the pertinent classification category(ies), or the number 1.5 plus the letter(s) that corresponds to that classification category(ies) listed in the following table.

Letter Category

A Military plans, weapons systems, or operations;

B Foreign government information;

C Intelligence activities (including special activities), intelligence sources or methods, or cryptology;

D Foreign relations or foreign activities of the United States, including confidential sources;

E Scientific, technological, or economic matters relating to the national security;

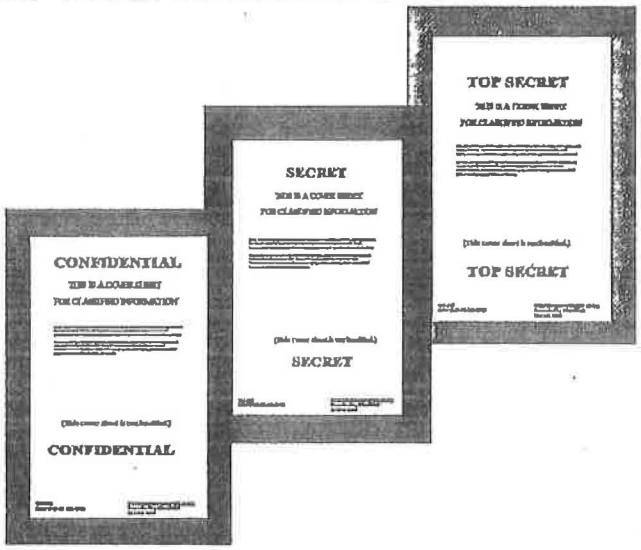
F United States Government programs for safeguarding nuclear materials or facilities; or

G Vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.

Declassification Instructions:

The duration of the original classification decision shall be placed on the "Declassify On" line.

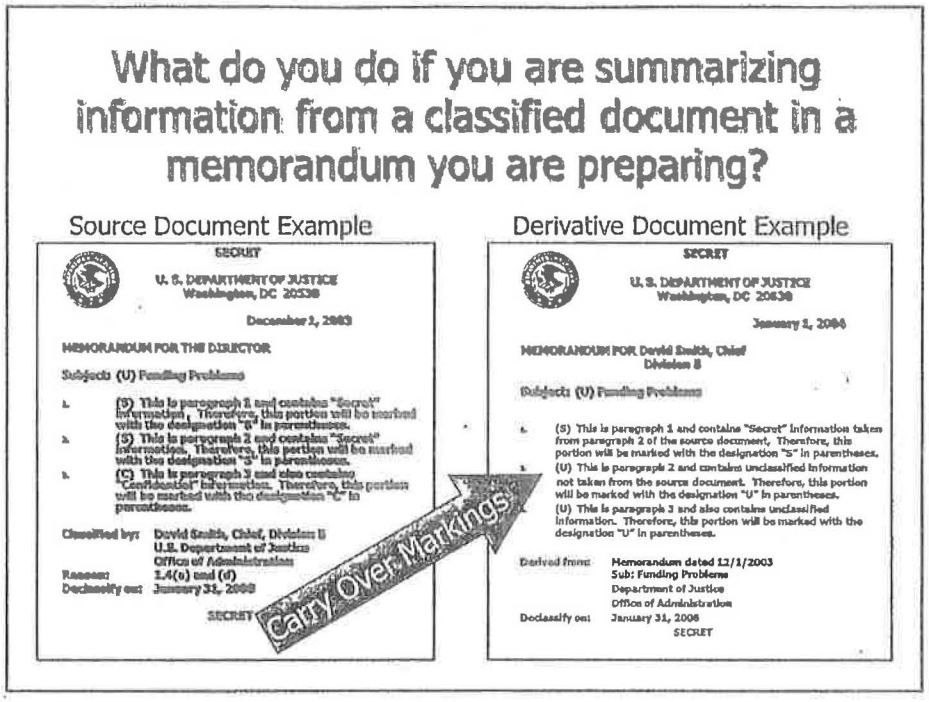
Marking Classified Information



All information and examples contained in this briefing are UNCLASSIFIED.

LIMITED OFFICIAL USE/UNCLASSIFIED

These are samples of the cover sheets. Blue identifies CONFIDENTIAL information, Red identifies SECRET information, and Orange identifies TOP-SECRET information.

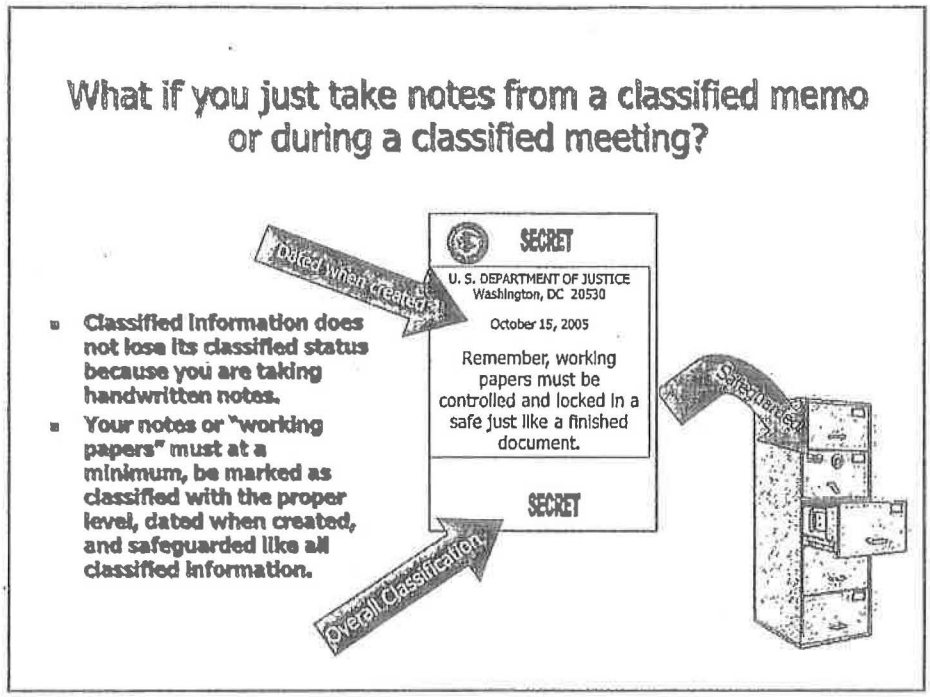


THIS SOURCE DOCUMENT IS ALSO AN EXAMPLE OF AN ORIGINALLY CLASSIFIED DOCUMENT.

THERE ARE SPECIFIC MARKING REQUIREMENTS FOR CLASSIFYING A DOCUMENT DERIVATIVELY, SO THAT IT IS PROPERLY PROTECTED LIKE THE ORIGINAL.

THE CLASSIFIED MARKINGS ON THE SOURCE DOCUMENT MUST BE CARRIED FORWARD TO YOUR DOCUMENT.

THE PORTIONS OF THE MEMO YOU ARE WRITING THAT ARE DERIVED FROM A CLASSIFIED DOCUMENT ARE ALSO CLASSIFIED AND MUST BE MARKED AS SUCH.



THIS SLIDE REFERS TO WORKING PAPERS. WHEN THOSE NOTES OR MEETING MINUTES BECOME A FINISHED DOCUMENT, YOU MUST MARK THEM ACCORDING TO SET PROCEDURES.

What are the procedures for processing classified information on a Laptop Computer System?

- **You must contact your Security Programs Manager (SPM) before a laptop computer can be used to process, store, or transmit classified information.**
- **A rules of behavior document will address the unique operating environment including authorized and official use; prohibitions; and changes to the system configuration.**
- **Any media produced by the system must be handled and stored in accordance with a Memorandum of Agreement (MOA) you and the SPM must sign.**

Accreditation must ensure that adequate security measures are in place to protect the information from compromise.

Keep a copy of the MOA with the system, especially during transport.

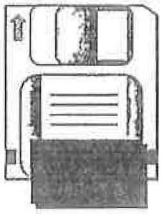
Carry a copy of the accreditation statement while on TDY.

What are the procedures for processing classified information on a Laptop Computer System? (Con't.)

- **Diskettes and removable drives must be labeled and secured in a GSA container or approved open storage area.**
- **Systems with non-removable disks and drives will require the entire system be stored in a GSA container or approved open storage area.**
- **Transporting a classified system will require that it be double wrapped in an opaque material, a courier letter/card from your SPM, and proper storage facilities at the off-site location.**

You must have a compelling operational need to process at approved areas while at a temporary duty (TDY) location.

Marking Diskettes, CDs and DVDs



Fold and wrap the classification label Around the bottom edge of the diskette.

Remember to mark the CD/DVD case too.

All information and examples contained in this briefing are UNCLASSIFIED.

LIMITED OFFICIAL USE/UNCLASSIFIED

There are similar label requirements for diskettes and CDs.

Transporting Classified Information

- **Two opaque sealed envelopes.**
- **Inner envelope properly addressed, including classification markings.**
- **Outer envelope properly addressed with no classification markings.**

All information and examples contained in this briefing are UNCLASSIFIED.

LIMITED OFFICIAL USE/UNCLASSIFIED

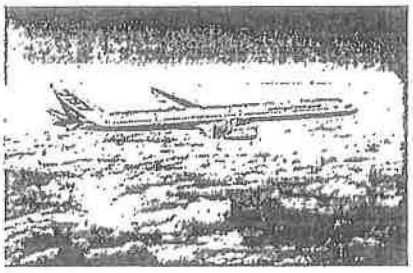
This next section goes into the appropriate **transmission of classified information.**

CONFIDENTIAL and SECRET material may be sent by U.S. Postal Service Registered Mail, Return Receipt Requested, or by U.S. Postal Service Overnight Express, Return Receipt Requested.

As you can see the inner envelope not only has the sender and recipient addresses, but also the classification labels.

The outer envelope is labeled the same, but does not include the classification labels.

Can you carry classified information onboard an aircraft?

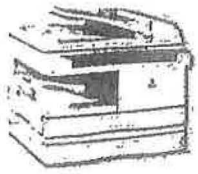


- **You must receive a courier briefing**
- **You can never leave classified material unattended**
- **You must travel directly to your destination**
- **You must arrange, in advance, for proper storage at your destination (can't keep it overnight in your hotel)**

1. POSSESS WRITTEN AUTHORITY: LETTER OR COURIER CARD
2. NOT READ OR DISPLAYED IN PUBLIC PLACES OR PUBLIC TRANSPORTATION.
3. TRANSPORT IN CARRY-ON LUGGAGE: NO METAL CLIPS!
4. TRAVEL DIRECTLY FROM OFFICE TO POINT OF DESTINATION.
5. RECIPIENT MUST HAVE CLEARANCE AND NEED-TO-KNOW. IF INTENDED RECIPIENT NOT THERE, MUST CHECK CLEARANCE OF PERSON TO ACCEPT, ALSO, AUTHORITY TO ACT AS RECIPIENT'S AGENT.
6. GET A RECEIPT.
7. LEAVE AN INVENTORY OF CONTENTS AND TRIP ITINERARY WITH THE ORIGINATING OFFICE IN THE EVENT OF LOSS OR THEFT.

Can you copy classified information on a photocopying machine?

- **Photocopy only on a designated machine**
- **You are responsible for ensuring that copying is not restricted by the persons who originated the information (ORCON – Originator Controlled)**
- **And, if you want someone else, for example, your secretary or assistant to copy information for you, they must have an appropriate security clearance**



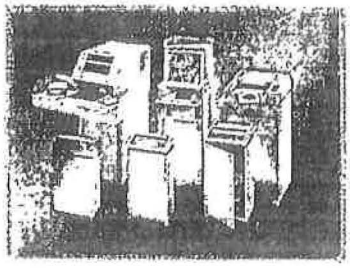
TYPICALLY, COPY MACHINES ARE TO BE OUT OF THE WAY OF MAINSTREAM PEDESTRIAN TRAFFIC, WHERE UNAUTHORIZED PERSONS CANNOT GAIN VISUAL ACCESS TO THE INFORMATION.

COPY MACHINES SHOULD NOT HAVE THE ABLITY TO RETAIN LATENT IMAGES.

Disposal of Classified Information

Classified material may be destroyed by:

- Burning
- Shredding
- Pulping
- Melting
- Mutilation
- Chemical Decomposition
- Pulverizing
- Degaussing



What ever method is used - You are personally responsible for ensuring that classified information is completely destroyed.

LIMITED OFFICIAL USE/UNCLASSIFIED

There are a variety of methods that may be used in the disposal of classified information.

Some of the more common methods are burning and shredding.

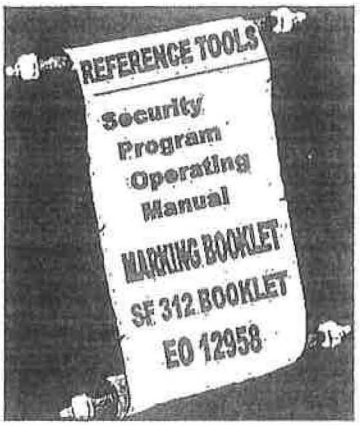
Whatever method is used, you are personally responsible for ensuring that the classified information in your custody is completely destroyed.

How do you know if someone is cleared to receive classified information?

- The Personnel Security Group or your Security Programs Manager can verify a DOJ employee's clearance status
- You may call (202) 616-7415 to get an employee's clearance
- Never rely on a person's own assertion that he or she has a security clearance
- Verifying clearances between agencies is always done from security office to security office – agai
  rely on a person's assurances

Available Tools

- **Every component has a Security Program Manager who can answer your questions and help you in many ways.**



LIMITED OFFICIAL USE/UNCLASSIFIED

There are a variety of resources available to you to help identify and/or implement appropriate security safeguards. Each component has their own Security Program Manager.

If all else fails and your component Security Program Manager is not available, you can always call the Security and Emergency Planning Staff (SEPS) for questions regarding safeguards or anything else in dealing with classified material.

There are also a number of reference documents available to you. For example the DOJ Security Program Operating Manual (SPOM), and "Executive Order 12958 as amended," to name a couple.

What if you make a mistake and don't properly safeguard classified information?

- **You must inform your Security Programs Manager (SPM) so that, for example, if you accidentally use your computer to word process classified information, the information can be erased from your hard drive**
- **Always report security lapses to your SPM so that the disclosure can be minimized**
- **There are sanctions for repeated failure to follow safeguarding measures that can include disciplinary action and/or revocation of your security clearance**
- **Sanctions are a last resort**

IN THE FINAL ANALYSIS-SECURITY IS AN INDIVIDUAL RESPONSIBILITY

YOUR SECURITY CLEARANCE CARRIES WITH IT A MOST IMPORTANT INDIVIDUAL RESPONSIBILITY—THE SAFEGUARDING OF CLASSIFIED INFORMATION VITAL TO THE SECURITY OF OUR NATION.

Recommended Reading

- Inside Terrorism Bruce Hoffman
- Inside Al Qaeda Rohan Gunaratna
- 9/11 Commission Report 9/11 Commision
- Terror in the Mind of God Mark Juergensmeyer
- The Cell John Miller
- The Crisis of Islam Bernard Lewis
- Terrorism and U.S. Foreign Policy Paul Pillar
- American Jihad Steve Emerson

Questions?