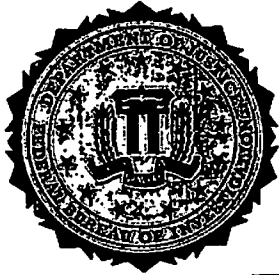


# USA PATRIOT Act Renewal



FBI Office of General Counsel  
National Security Law Branch  
202-324-3951

Last updated 31 March 2006.

Certain materials in this presentation are included pursuant to the fair use exemption of the U.S. Copyright Laws.

Unclassified



# Test

- USA PATRIOT Act is an acronym.
- Who can give me the full title?



# Answer

- "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001"

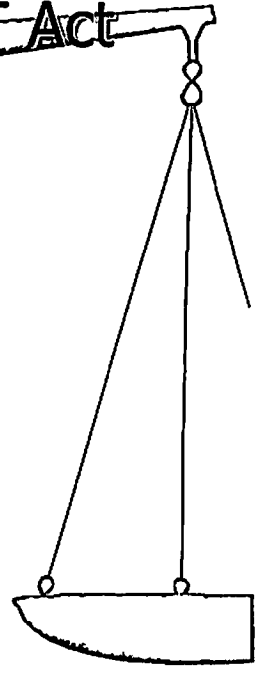


March 9, 2006

President renewed the USA PATRIOT Act  
2001

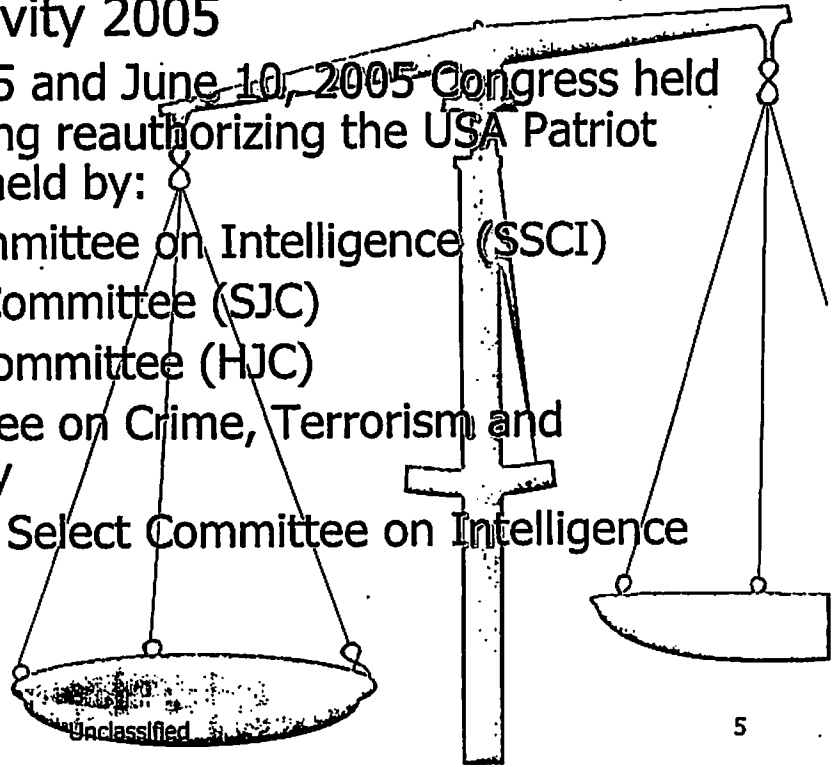


Unclassified



# USA PATRIOT Act 2001 Renewal Debate

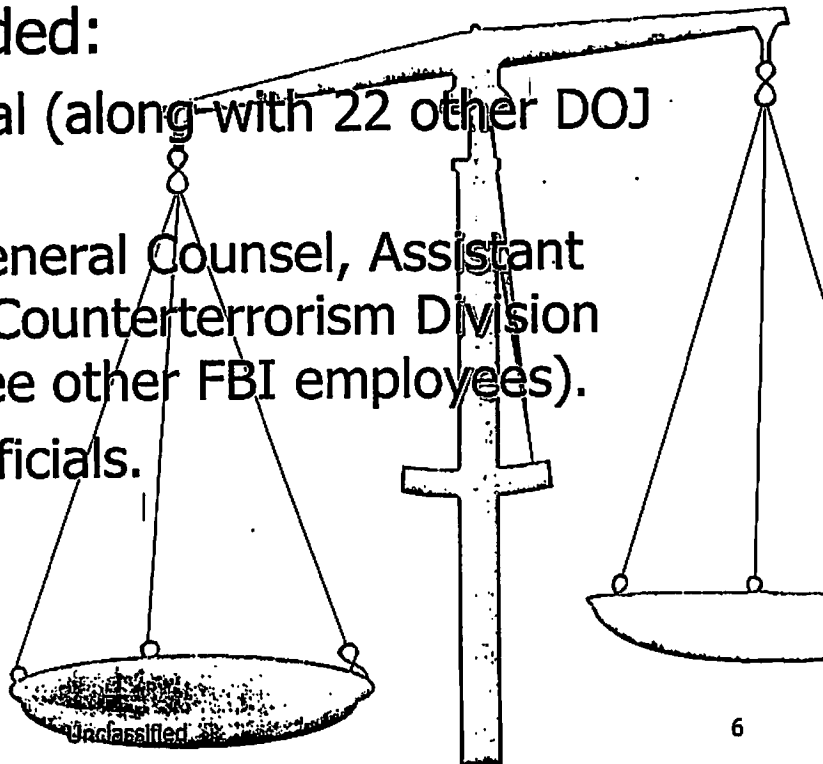
- Congressional Activity 2005
- Between April 5, 2005 and June 10, 2005 Congress held 18 hearings concerning reauthorizing the USA Patriot Act. Hearings were held by:
  - Senate Select Committee on Intelligence (SSCI)
  - Senate Judiciary Committee (SJC)
  - House Judiciary Committee (HJC)
  - HJC's Subcommittee on Crime, Terrorism and Homeland Security
  - House Permanent Select Committee on Intelligence (HPSCI)



# USA PATRIOT Act 2001 Renewal Debate

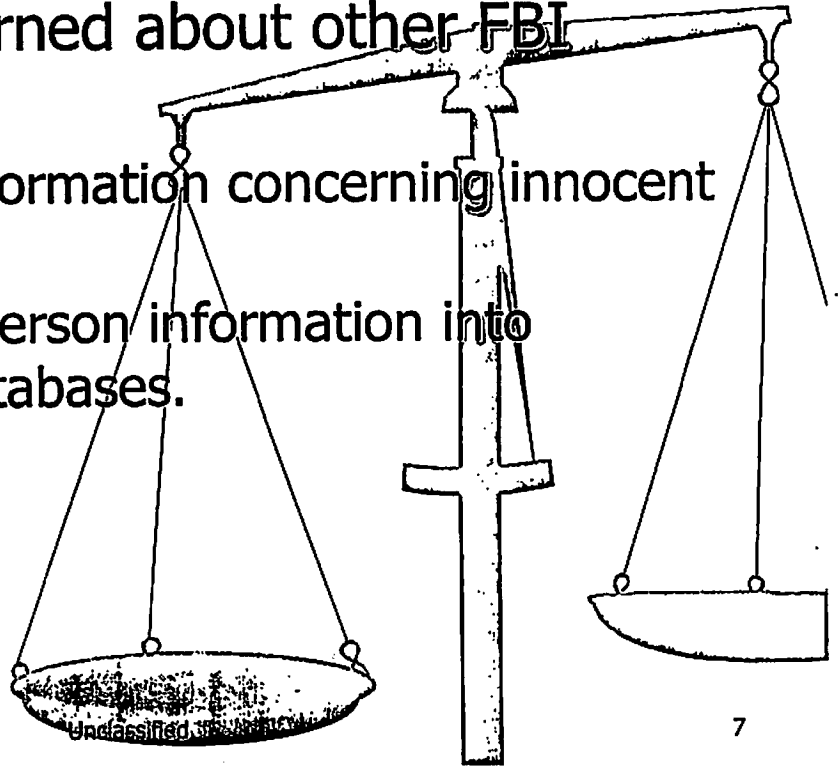
## ■ Witnesses included:

- Attorney General (along with 22 other DOJ employees).
- FBI Director, General Counsel, Assistant Director of the Counterterrorism Division (along with three other FBI employees).
- NSA and CIA officials.



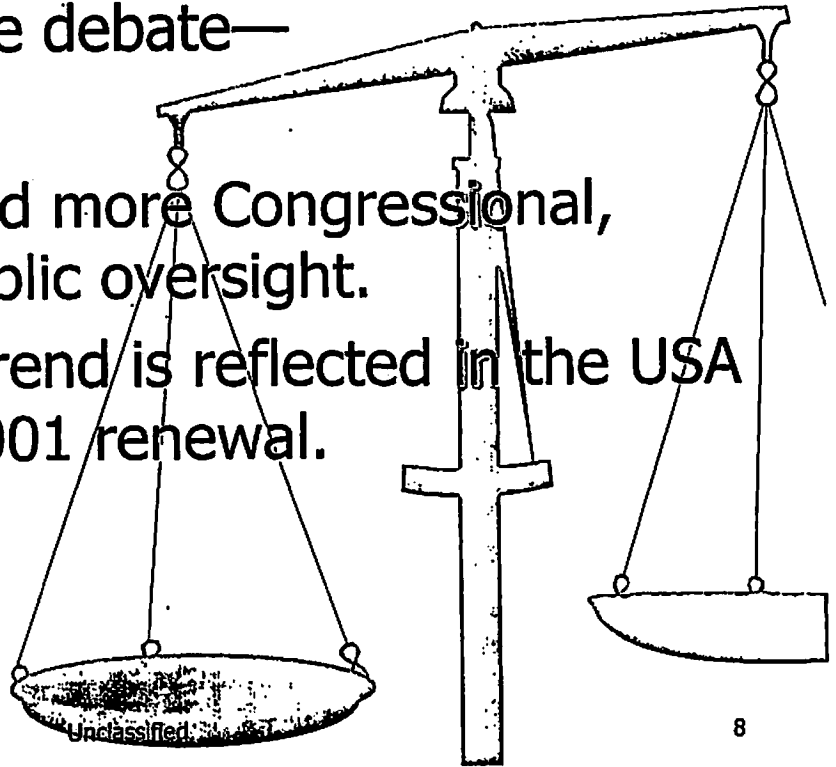
# USA PATRIOT Act 2001 Renewal Debate

- Congress concerned about other FBI activities --
  - Collection of information concerning innocent citizens.
  - Deposit of US Person information into government databases.
  - Data-mining.



# USA PATRIOT Act 2001 Renewal Debate

- Trend during the debate—
- Congress wanted more Congressional, Judicial, and Public oversight.
- This oversight trend is reflected in the USA PATRIOT Act 2001 renewal.





# USA PATRIOT Act 2001 Renewal

Actually required 2 new Public Laws to accomplish

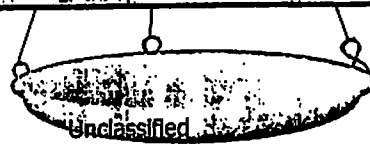
Public Law 109-177

Public Law 109-178

USA PATRIOT  
Improvement and  
Reauthorization Act  
of 2005

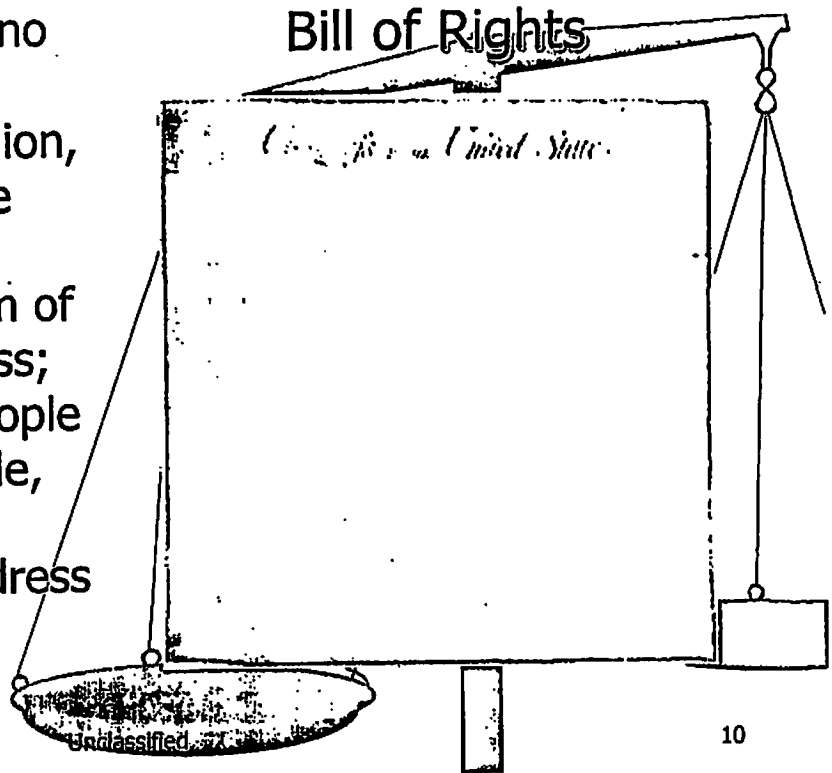
"USA PATRIOT IRA"

USA PATRIOT Act  
Additional  
Reauthorizing  
Amendments Act of  
2006.



# 1<sup>st</sup> Amendment

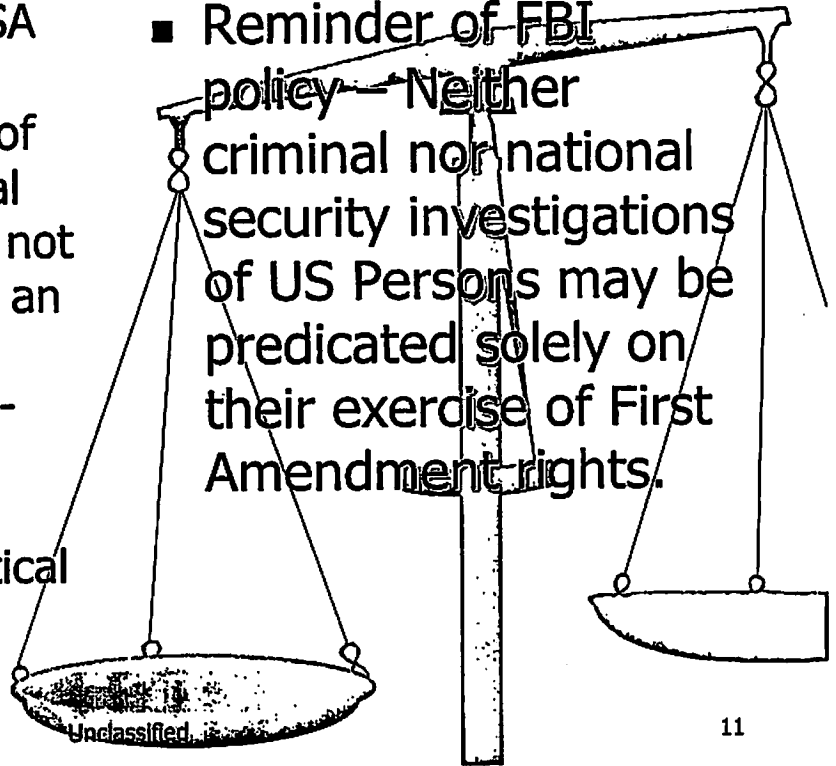
- Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.



# 1<sup>st</sup> Amendment

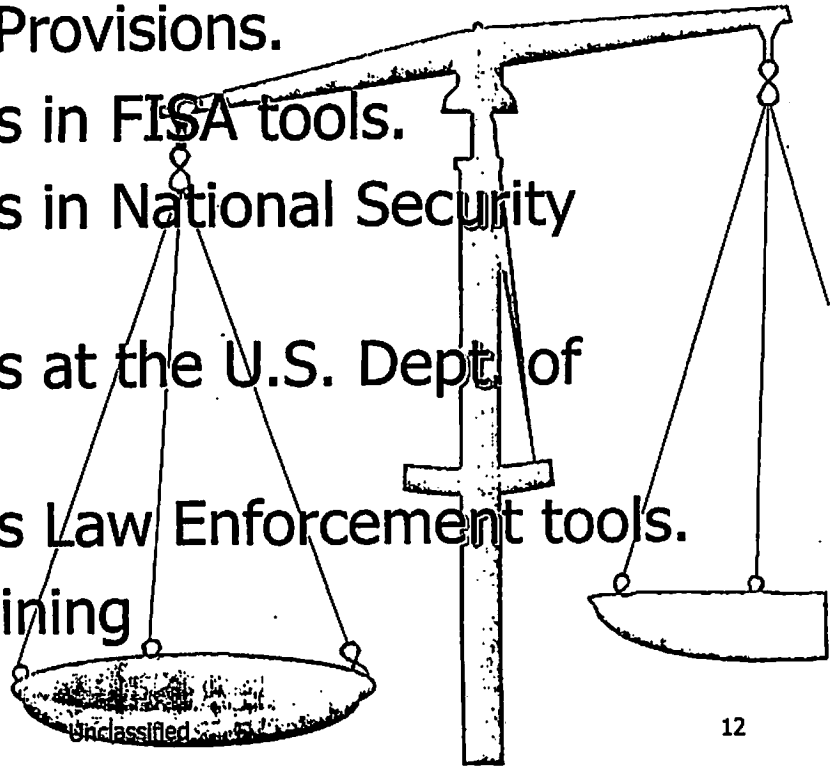
- Section 124 of the USA PATRIOT IRA 2005 – expressed the sense of Congress that “federal investigations should not be based solely upon an American citizen’s membership in a non-violent political organization or their otherwise lawful political activity.”

- Reminder of FBI policy – Neither criminal nor national security investigations of US Persons may be predicated solely on their exercise of First Amendment rights.



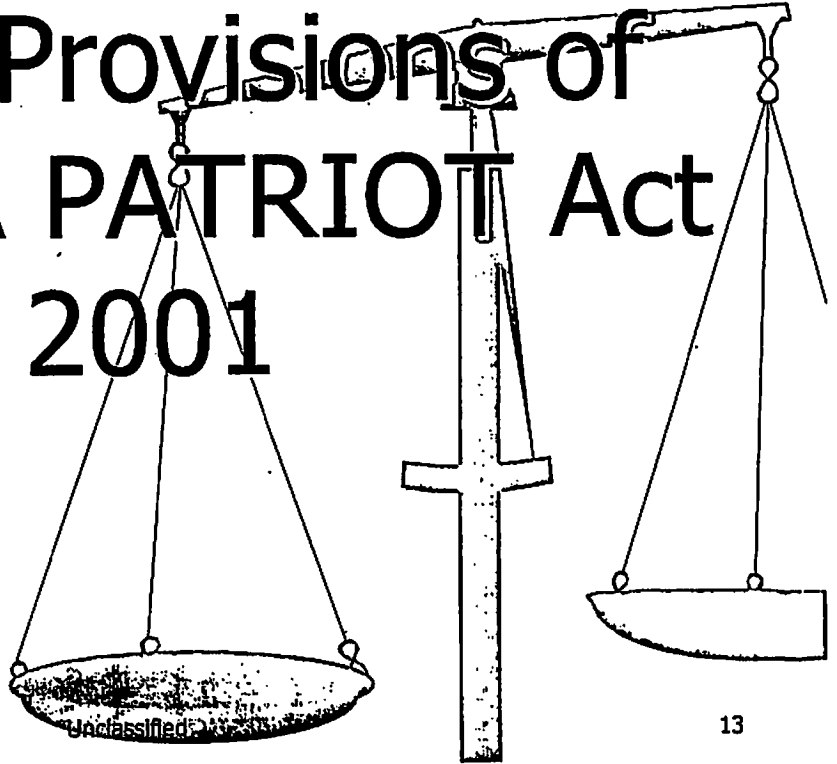
# Will cover changes in the new laws as follows:

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



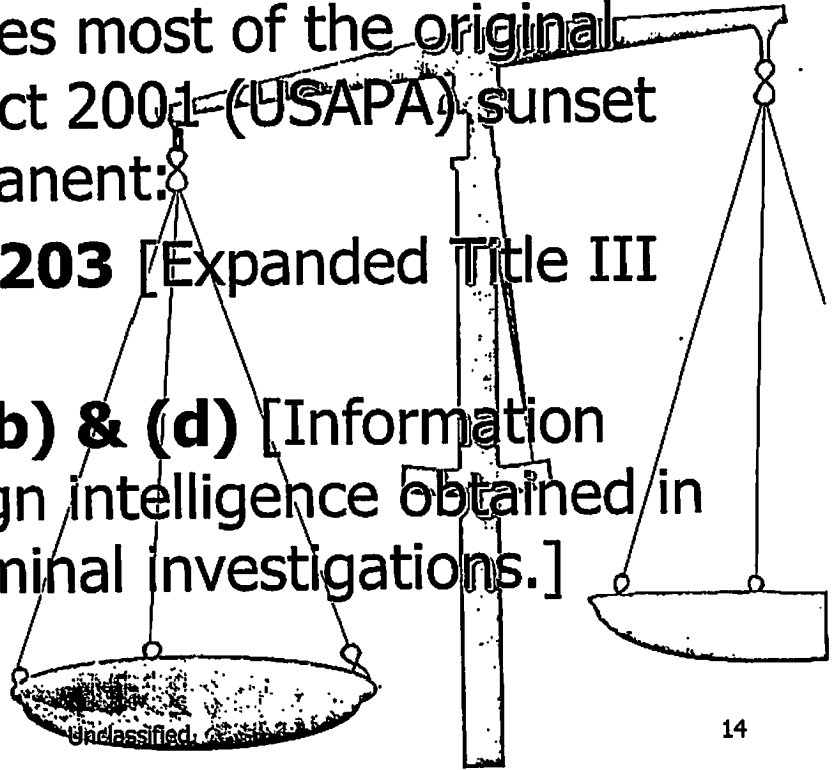
# Part 1

# Sunset Provisions of the USA PATRIOT Act 2001



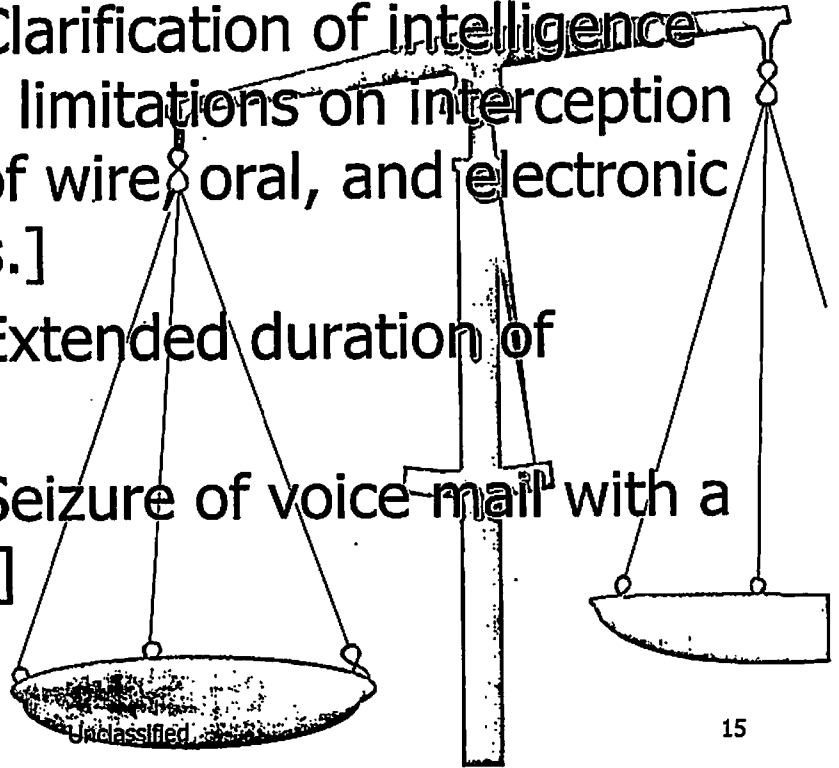
# USA PATRIOT Act 2001 Sunset Provisions - Permanent

- USAPA IRA makes most of the original USA PATRIOT Act 2001 (USAPA) sunset provisions permanent:
- **Sections 201/203** [Expanded Title III predicates.]
- **Sections 203(b) & (d)** [Information sharing of foreign intelligence obtained in Title III and criminal investigations.]



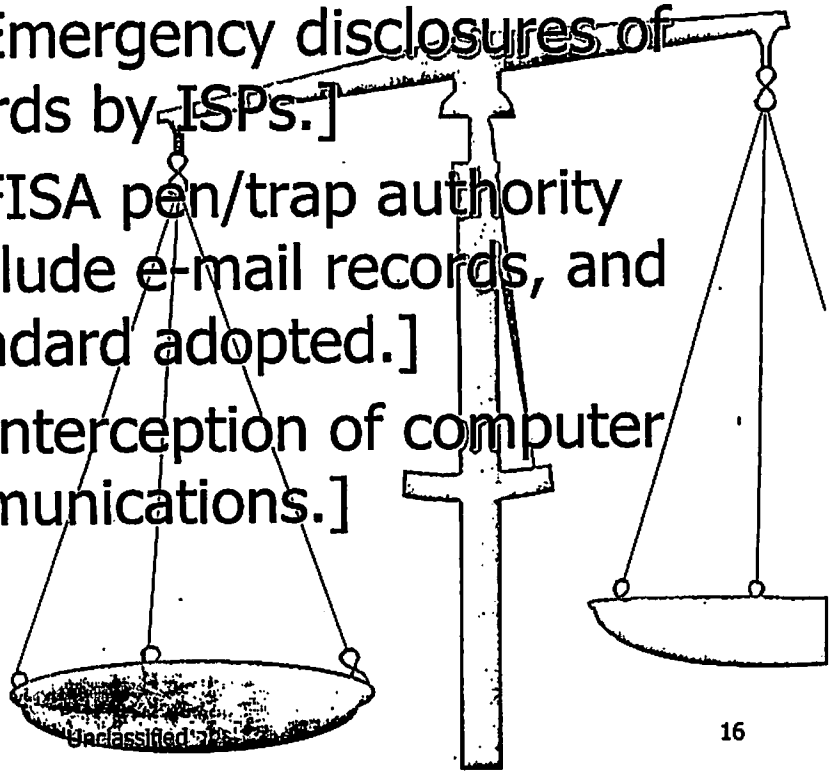
# USA PATRIOT Act 2001 Sunset Provisions - Permanent

- **Section 204** [Clarification of intelligence exceptions from limitations on interception and disclosure of wire, oral, and electronic communications.]
- **Section 207** [Extended duration of certain FISAs.]
- **Section 209** [Seizure of voice mail with a search warrant.]



# USA PATRIOT Act 2001 Sunset Provisions - Permanent

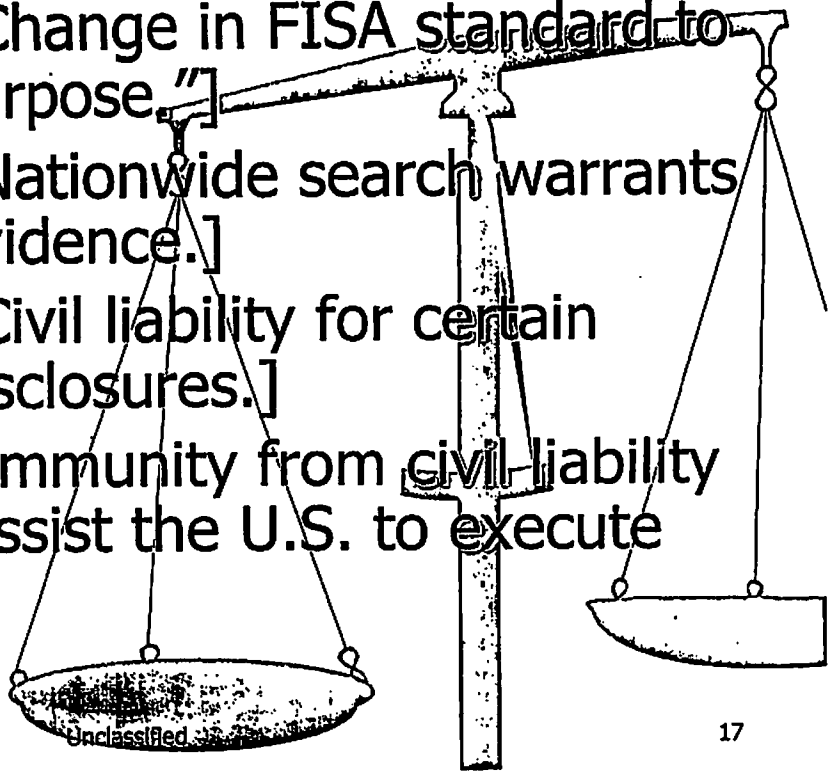
- **Section 212** [Emergency disclosures of e-mail and records by ISPs.]
- **Section 214** [FISA pen/trap authority expanded to include e-mail records, and "relevance" standard adopted.]
- **Section 217** [Interception of computer trespasser communications.]





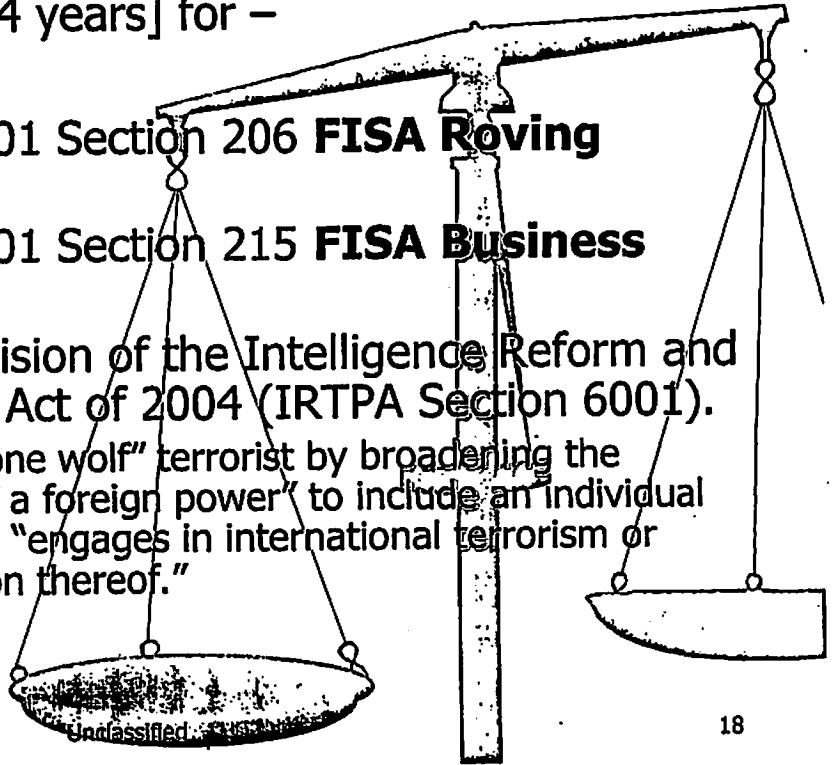
# USA PATRIOT Act 2001 Sunset Provisions - Permanent

- **Section 218** [Change in FISA standard to "a significant purpose."]
- **Section 220** [Nationwide search warrants for electronic evidence.]
- **Section 223** [Civil liability for certain unauthorized disclosures.]
- **Section 225** [Immunity from civil liability for those who assist the U.S. to execute FISA wiretaps.]



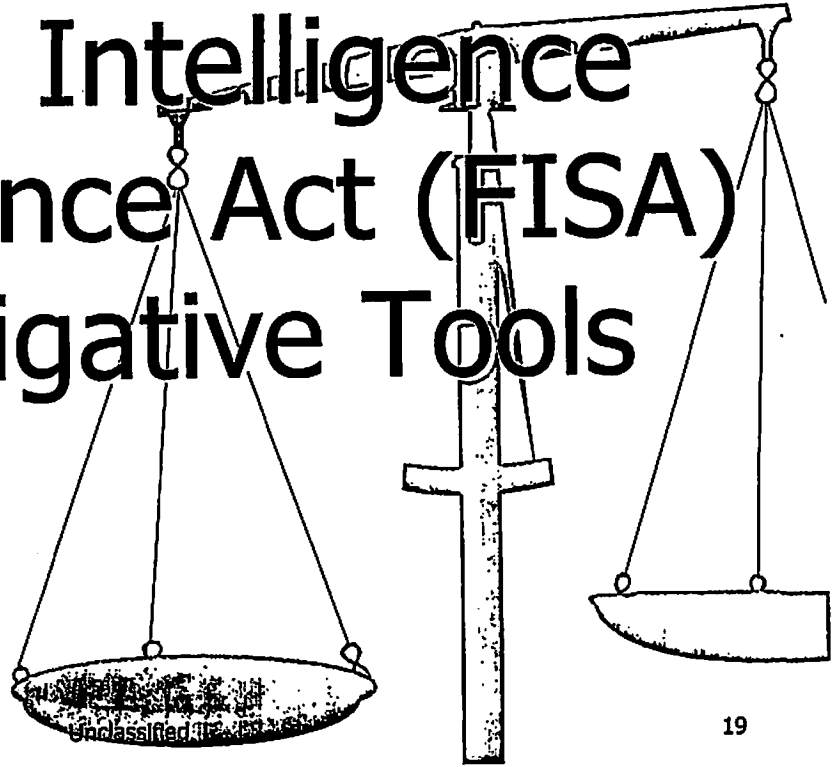
# New Sunset Provisions

- December 31, 2009 [4 years] for –
- USA PATRIOT Act 2001 Section 206 **FISA Roving surveillance.**
- USA PATRIOT Act 2001 Section 215 **FISA Business Records.**
- FISA "lone wolf" provision of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA Section 6001).
  - This addressed the "lone wolf" terrorist by broadening the definition of "agent of a foreign power" to include an individual other than a USP who "engages in international terrorism or activities in preparation thereof."



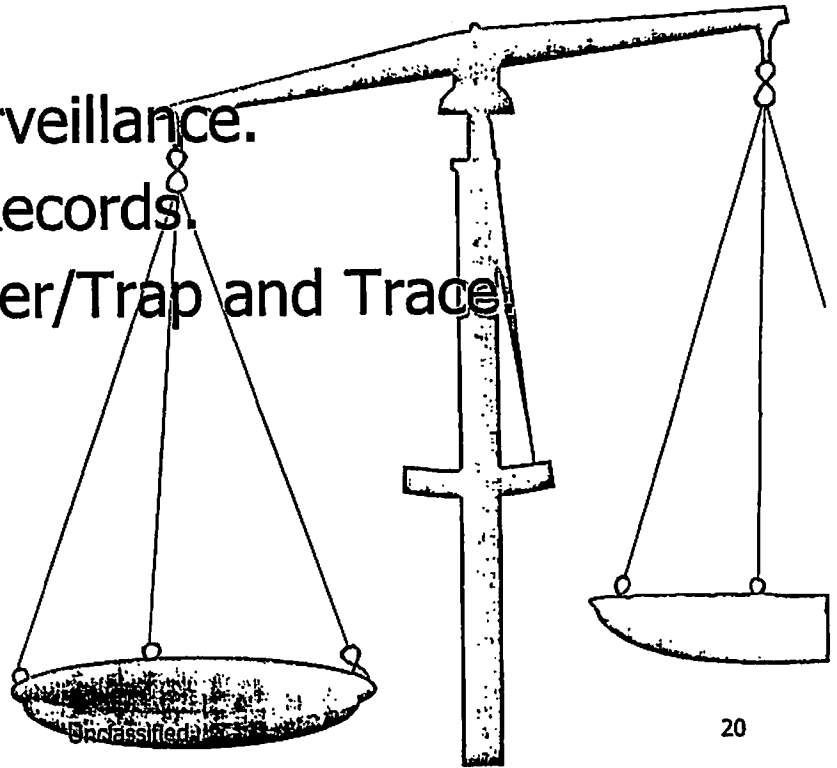
## Part 2

# Foreign Intelligence Surveillance Act (FISA) Investigative Tools



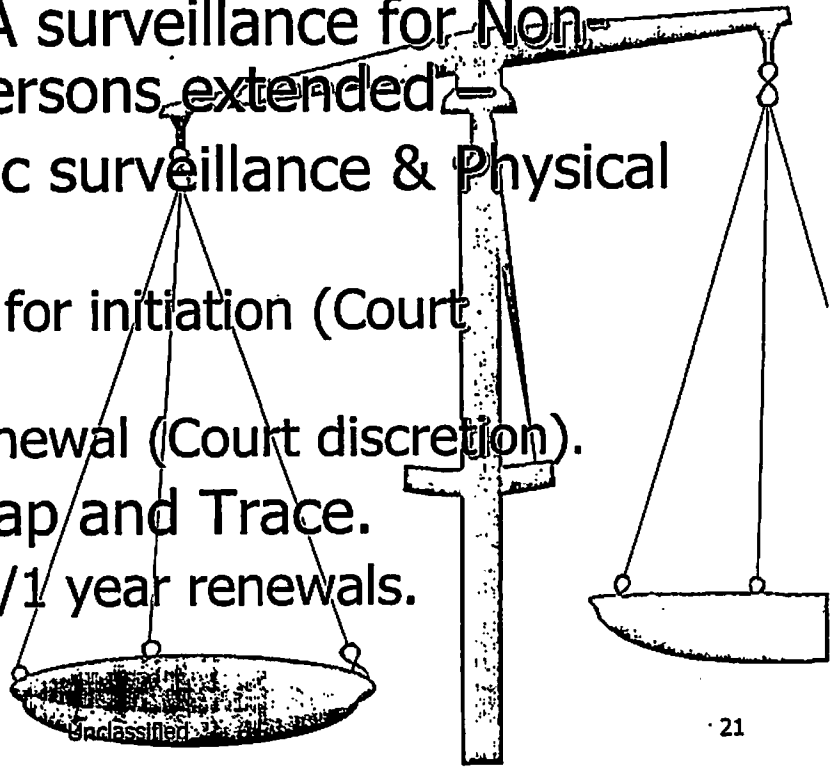
# Changes to FISA Tools

- FISA Durations.
- FISA Roving Surveillance.
- FISA Business Records.
- FISA Pen Register/Trap and Trace.
- FISA Oversight.



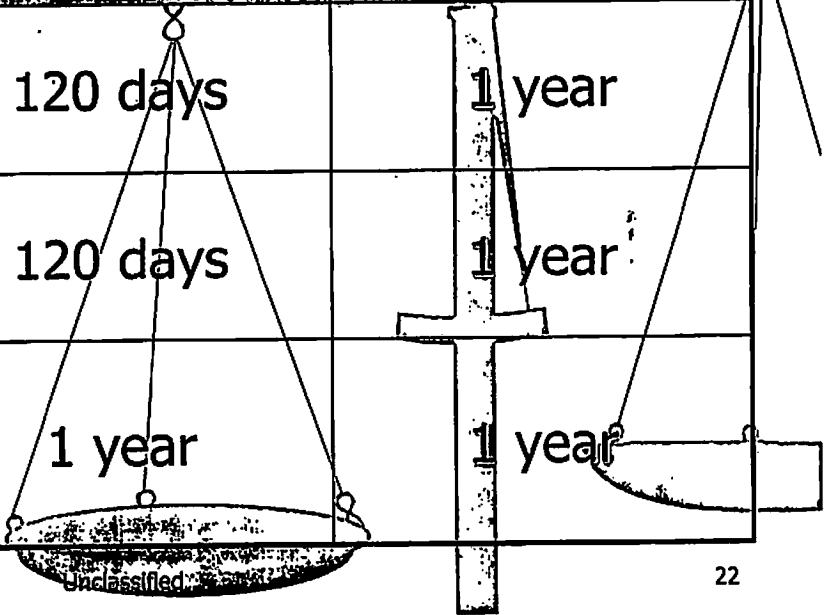
# FISA Duration

- Duration of FISA surveillance for Non-United States Persons extended.
- Covers electronic surveillance & Physical Search.
  - Up to 120 days for initiation (Court discretion).
  - Up to 1 year renewal (Court discretion).
- Pen Register/Trap and Trace.
  - 1 year initiation/1 year renewals.



# FISA Duration

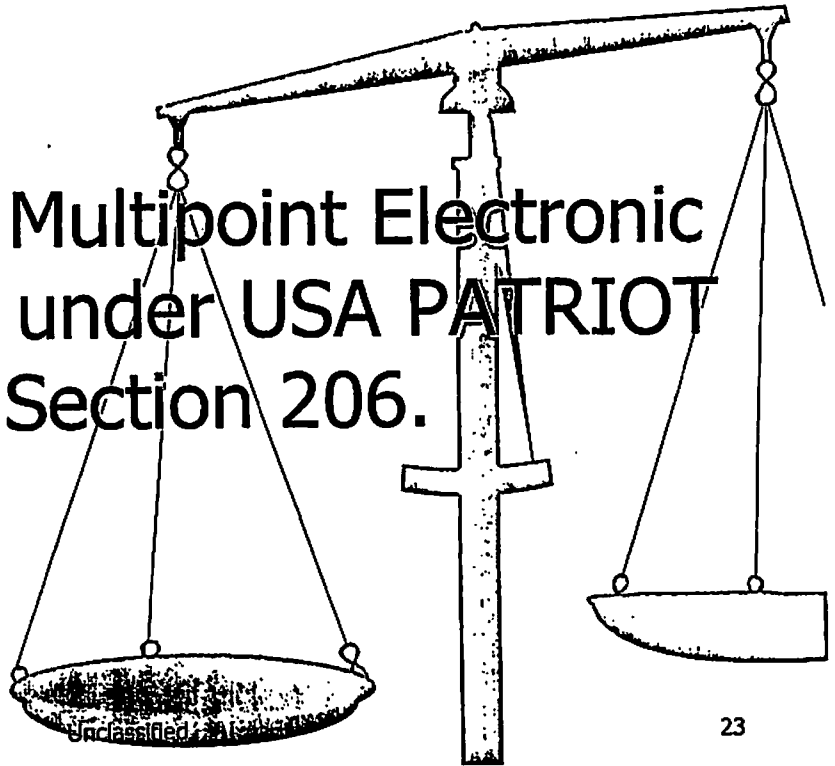
| FISA Technique                    | Non-USP<br>Initiations | Non-USP<br>Renewals |
|-----------------------------------|------------------------|---------------------|
| Electronic<br>Surveillance        | 120 days               | 1 year              |
| Physical Search                   | 120 days               | 1 year              |
| Pen<br>register/Trap<br>and Trace | 1 year                 | 1 year              |



Unclassified

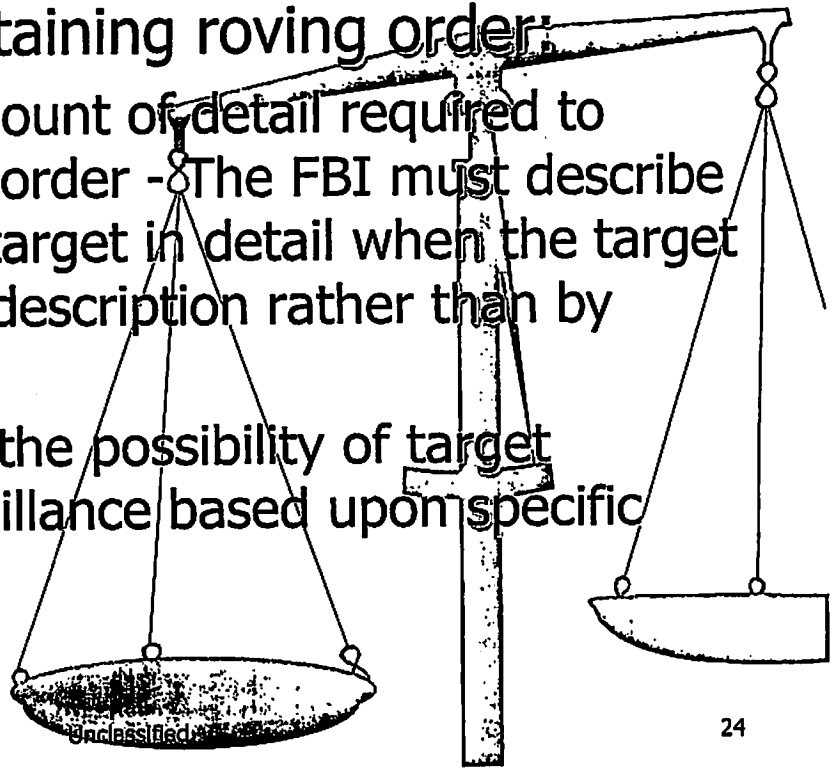
# FISA Roving Surveillance

- Changes to Multipoint Electronic Surveillance under USA PATRIOT Act Section 206.



# FISA Roving Surveillance

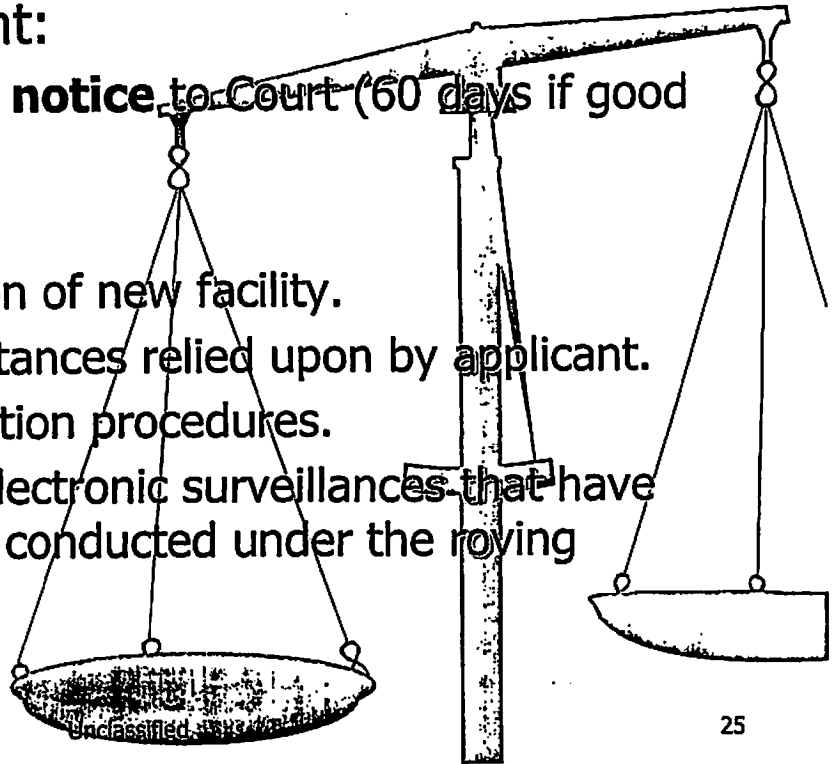
- Standard for obtaining roving order:
  - Clarified the amount of detail required to obtain a roving order - The FBI must describe the "**specific**" target in detail when the target is identified by description rather than by name.
  - FISC must find the possibility of target thwarting surveillance based upon specific facts.





# FISA Roving Surveillance

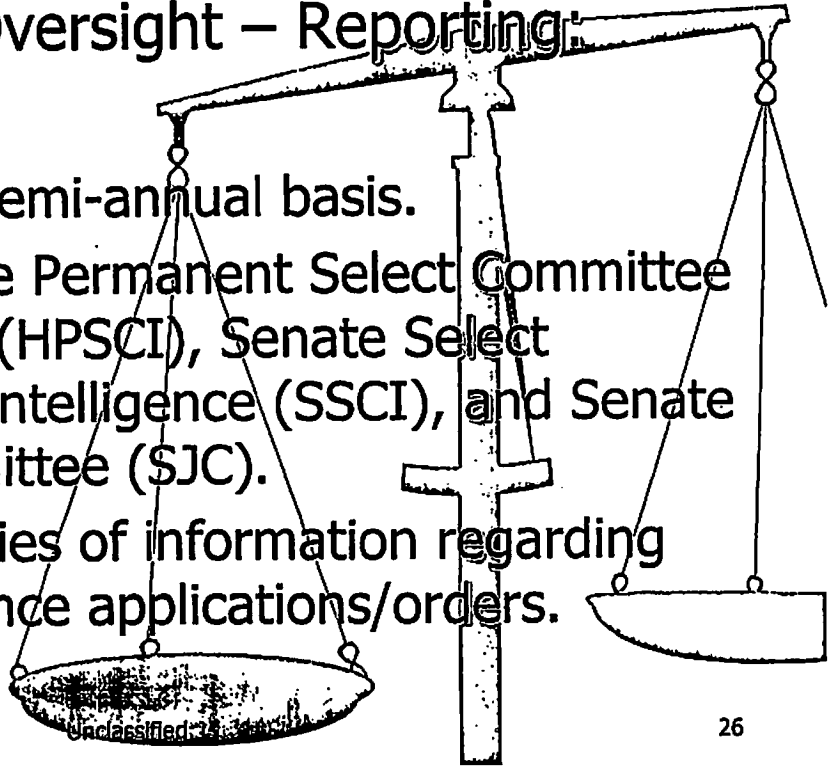
- Return requirement:
  - Presumed **10 day notice** to Court (60 days if good cause).
- Report to Court—
  - Nature and location of new facility.
  - Facts and circumstances relied upon by applicant.
  - Any new minimization procedures.
  - Total number of electronic surveillances that have been or are being conducted under the roving authority.



# FISA Roving Surveillance

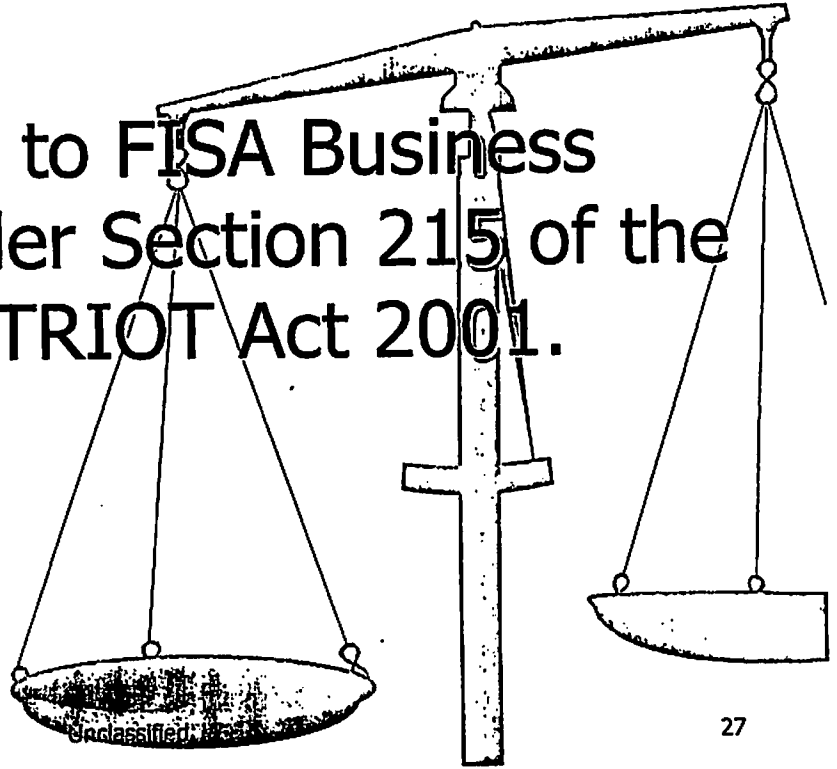
## ■ Congressional Oversight – Reporting:

- AG reports on semi-annual basis.
- Report to House Permanent Select Committee on Intelligence (HPSCI), Senate Select Committee on Intelligence (SSCI), and Senate Judiciary Committee (SJC).
- Several categories of information regarding roving surveillance applications/orders.



# FISA Business Records

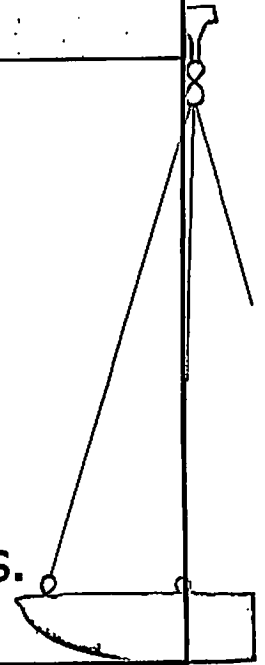
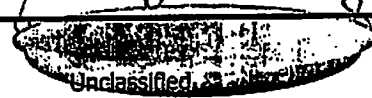
- Changes to FISA Business Records Under Section 215 of the USA PATRIOT Act 2001.



# FISA Business Records

## Highlights

- New "presumptive relevance" test.
- Special categories of tangible things.
- Recipient challenge/Judicial review.
- Minimization procedures w/i 180 days.

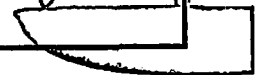
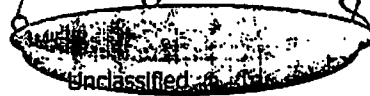


# FISA Business Records

## Scope of FISA Business Records authority

This authority may be used to obtain **"any tangible things (including books, records, papers, documents, and other items."**

- Broad – similar in scope to a Federal grand jury subpoena.
- The scope of this authority has not been changed.



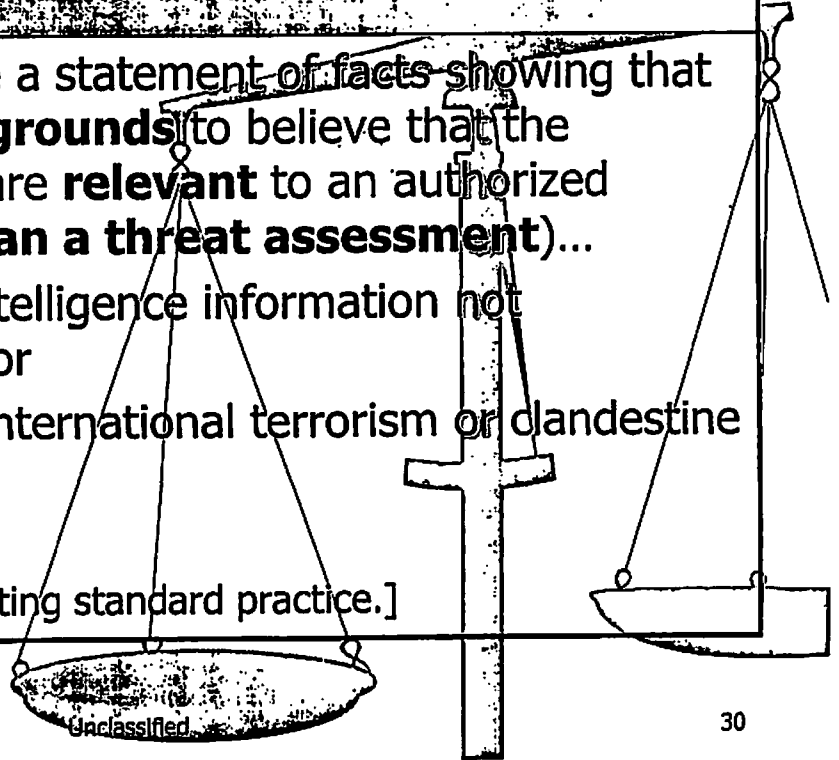
# FISA Business Records

## Standard = Relevance

Application shall include a statement of facts showing that there are **reasonable grounds** to believe that the tangible things sought are **relevant** to an authorized investigation (**other than a threat assessment**)...

- to obtain foreign intelligence information not concerning US person, or
- to protect against international terrorism or clandestine intelligence activities...

[This makes explicit the existing standard practice.]



# FISA Business Records

## New Presumptive Relevance Test

The tangible things are **presumptively relevant** if the facts show they pertain to –

- (i) a foreign power or an agent of a foreign power;
- (ii) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation, or
- (iii) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation.

[These cases probably cover most situations.]

unclassified

# FISA Business Records

**FISA  
Business  
Records  
Order must  
comply with  
the following:**

- Describe the tangible things with **sufficient particularity** to permit them to be fairly identified.
- Contain a **date of return**.
- Date must give recipient **reasonable period of time** to produce.
- May only require the production of tangible things that would be available with a GJ subpoena or a District Court order [this maintains privileges (ex.: attorney/client)].

Unclassified



# FISA Business Records

| Special Categories of Tangible Things require Special Approval and Procedures |  |
|---|--|
| Special Categories:   | <ul style="list-style-type: none"><li>•Library circulation records and Library patron lists.</li><li>•Book sales records and Book customer lists.</li><li>•Firearm sales records.</li><li>•Tax return information.</li><li>•Educational records.</li><li>•Medical records.</li></ul> |
| Special Approval Level:   | The <b>Director, the Deputy Director, or the Executive Assistant Director for National Security</b> must make the application for special categories of tangible things that contain information that would identify a person.   |

Unclassified

# FISA Business Records

| Special Categories of Tangible Things require Special Approval and Procedures |   |
|---|---|
| Congressional Reporting:  | AG must report annually on Special Categories to HPSCI, HJC, SSCI, and SJC.   |
| Note:   | Approval authority for all FISA Business Record requests (except special categories): <ol style="list-style-type: none"><li>1. Deputy Director;</li><li>2. EAD and associate EAD for the NSD;</li><li>3. the Assistant Director and all Deputy Assistant Directors of Counterterrorism, Counterintelligence, and Cyber Divisions;</li><li>4. the General Counsel, and the DGC for the National Security Law Branch.</li></ol> |

Unclassified

# FISA Business Records

|                      |  |
|----------------------|--|
| <b>Nondisclosure</b> | No person shall disclose the fact that the FBI has sought tangible things [same as before].  |
| <b>Exceptions</b>    | Recipient may disclose order to –<br>(1) Persons to whom disclosure is necessary to comply [same as before];<br>(2) An attorney to obtain legal advice or assistance with respect to the production [new provision made explicit what had been implicit];<br>(3) A person a permitted by the Director (or designee). |

Unclassified

# FISA Business Records

## Extension of nondisclosure to others:

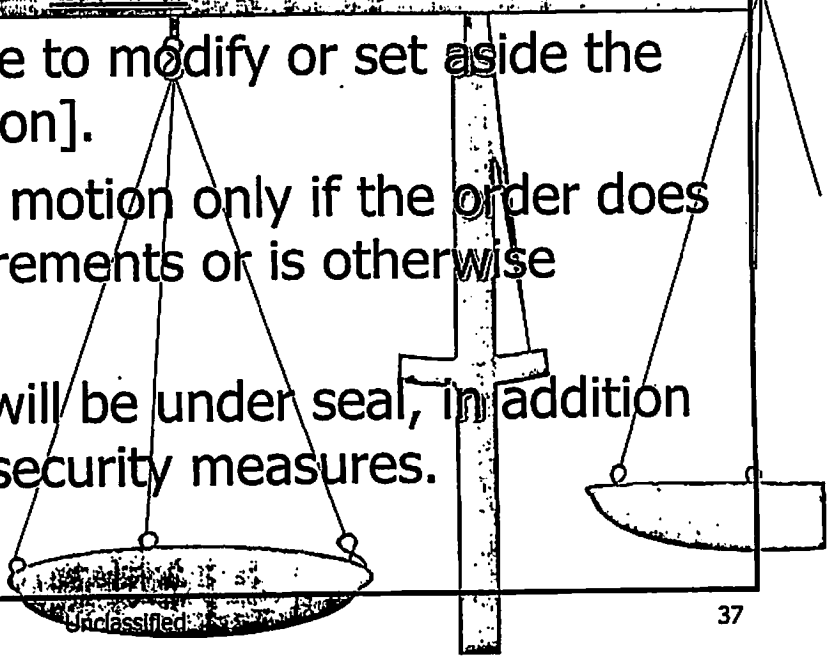
- Recipient shall notify the person of the nondisclosure.
- Person shall be subject to the nondisclosure.
- Director (or designee) may ask the recipient to identify the other persons to whom disclosure made **(except that the recipient does not have to identify the attorney)**.

Unclassified

# FISA Business Records

## Recipient's Challenge of FISA Business Records Order

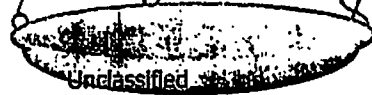
- Recipient may move to modify or set aside the order [FISC jurisdiction].
- FISC may grant the motion only if the order does not meet FISA requirements or is otherwise unlawful.
- Security: All filings will be under seal, in addition to FISC established security measures.



Unclassified

# FISA Business Records

| <u>Recipient's Challenge of Nondisclosure provision</u> |   |
|---|---|
| Timing:   | Not less than 1 year after order – recipient may move to modify or set aside the nondisclosure order.   |
| FISA Court (FISC)                                       | FISC may grant only if, based on the government's application and recipient's petition, no reason to believe that disclosure –<br><b>may endanger the national security of the U.S., interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person.</b> |

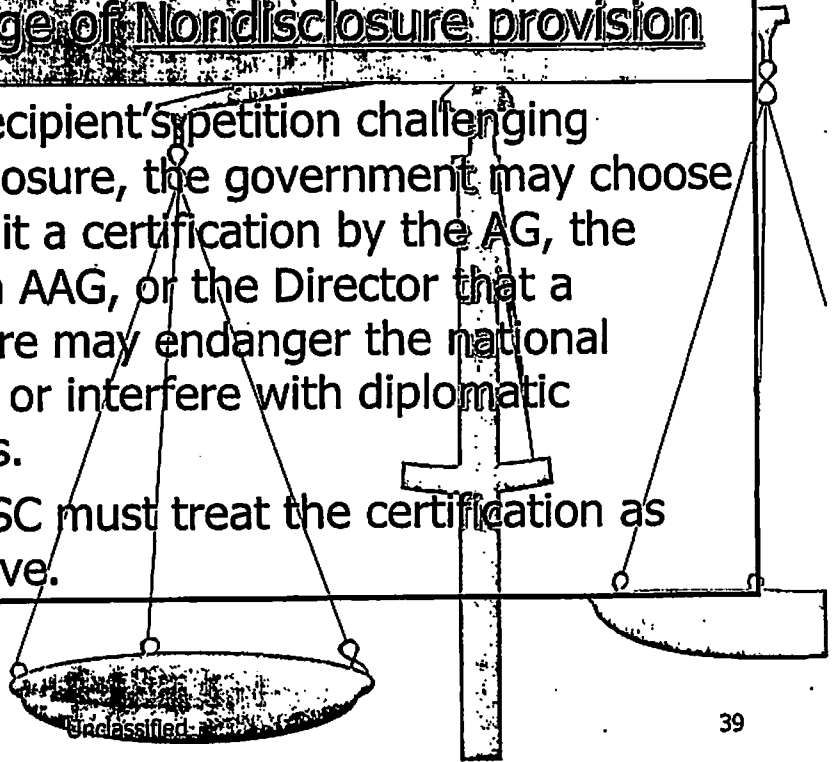


# FISA Business Records

## Recipient's Challenge of Nondisclosure provision

### Conclusive Certification

- After recipient's petition challenging nondisclosure, the government may choose to submit a certification by the AG, the DAG, an AAG, or the Director that a disclosure may endanger the national security or interfere with diplomatic relations.
- The FISC must treat the certification as conclusive.



# FISA Business Records

## Minimization Procedures

- W/in 180 days of enactment (approx 9/9/2006).
- AG shall adopt minimization procedures to govern the retention and dissemination of information.
- Minimize the retention/Prohibit the dissemination:
  - Nonpublicly available info re unconsenting USPs
  - Consistent with the US IC need to obtain, produce and disseminate foreign intelligence information.
- Evidence of a Crime: Procedures should allow for the retention and dissemination of this information.

Unclassified



# FISA Business Records

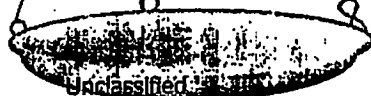
## Oversight – Congressional/Public Reporting

•AG to report annually (April) to HPSCI, HJC, SSCI & SJC.

•Report on

- (1) total # of FISA BR applications,
- (2) total # of orders granted, modified, or denied, and
- (3) total # orders granted, modified, or denied for special categories.

•AG to make an **unclassified annual report** (April) on the total # of FISA BR applications and total # of orders granted, modified, or denied (gives the public a view of activities).



# FISA Business Records

| DOJ IG Comprehensive Audit of FISA BRs         |  |
|--|--|
| Scope & Timing                                 | Comprehensive audit of effectiveness (including any improper or illegal use) covering 2002 to 2006.<br>▪Report to HSPCI, HJC, SSCI and SJC.  |
| Effectiveness of FISA BRs Process (including): | ▪How often FBI requested DOJ OIPR to submit an application and the request was not submitted (and why?).<br>▪Justification for the failure of AG to issue implementing procedures in a timely fashion, and whether the delay harmed national security.<br>▪Whether bureaucratic or procedural impediments prevent the FBI from fully using the tool. |

Unclassified

# FISA Business Records

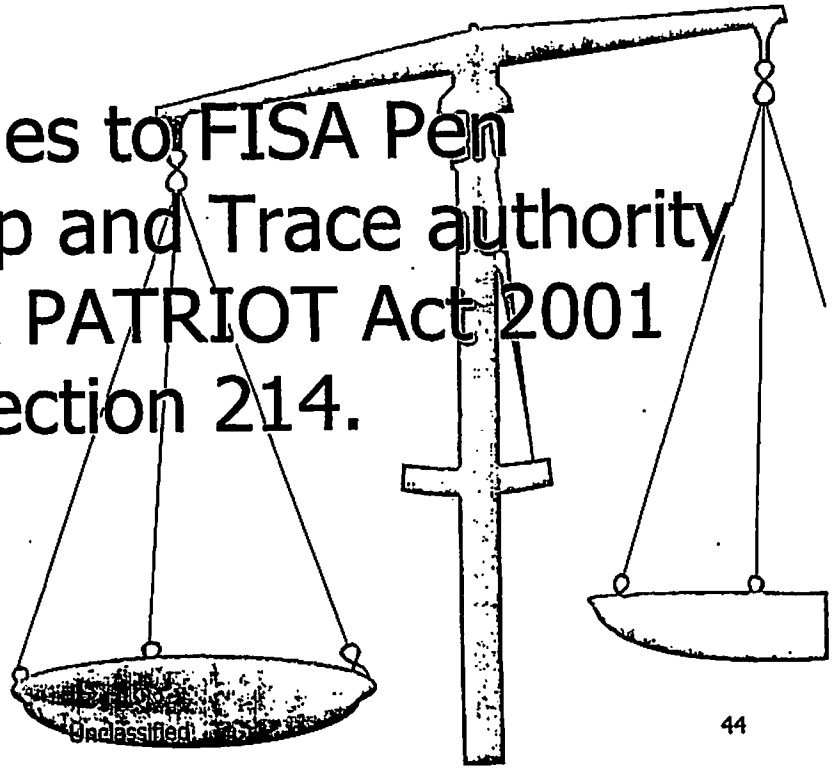
## DOJ IG Comprehensive Audit of FISA BRs

Effectiveness of  
FISA BRs  
(including):

- Categories of info obtained and the importance of the info to the FBI and the IC.
- How info is collected, retained, analyzed, and disseminated by the FBI (including access of "raw data" to other agencies of the Federal, state, local, or tribal governments, or private sector entities).
- Minimization procedures adopted by AG.
- Whether/how often FBI used info to produce analytical intelligence products for the FBI, the IC, or other agencies of the federal, state, local or tribal governments.
- Whether/how often FBI provided info to law enforcement for criminal proceedings.

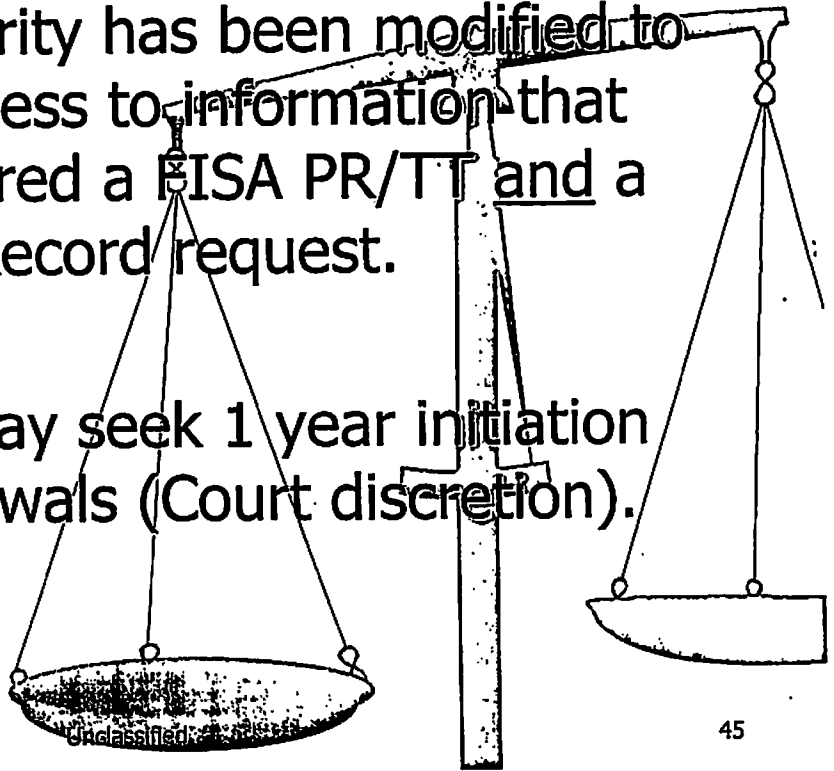
# FISA Pen Register/Trap and Trace

- Changes to FISA Pen Register/Trap and Trace authority under USA PATRIOT Act 2001 Section 214.



# FISA Pen Register/Trap and Trace

- This FISA authority has been modified to give the FBI access to information that previously required a FISA PR/TT and a FISA Business Record request.
- For non-UPS, may seek 1 year initiation and 1 year renewals (Court discretion).

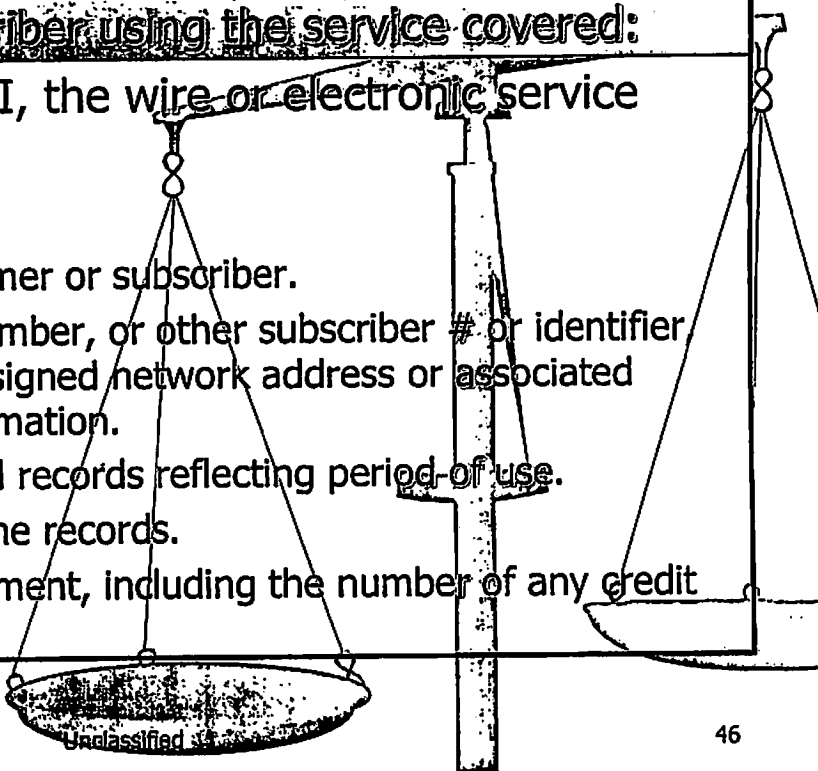


# FISA Pen Register/Trap and Trace

## Customer or Subscriber using the service covered:

At the request of the FBI, the wire or electronic service shall disclose –

- Name and address of customer or subscriber.
- Telephone or instrument number, or other subscriber # or identifier including any temporarily assigned network address or associated routing or transmission information.
- Length/Types of service and records reflecting period of use.
- Local/long distance telephone records.
- Mechanisms/sources of payment, including the number of any credit card or bank account used.



# FISA Pen Register/Trap and Trace

Customer or Subscriber of Incoming/outgoing communications to/from the service covered:

At the request of the FBI, the wire or electronic service shall disclose –

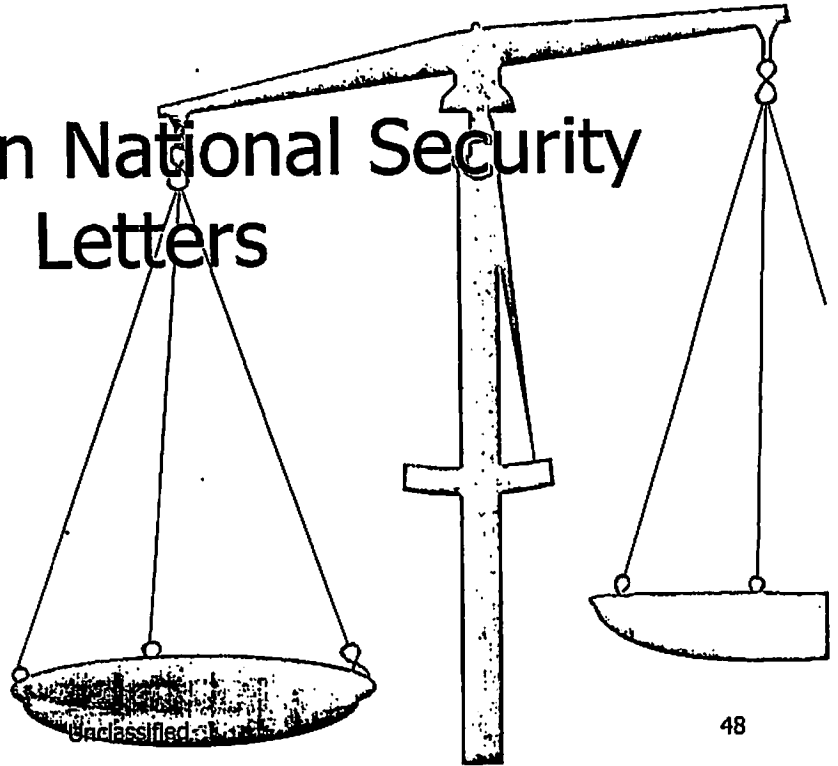
- Name/address of customer or subscriber.
- Telephone or instrument number, or other subscriber number or identifier, including any temporarily assigned network address or associated routing or transmission information.
- Length/Types of service.

[Subscriber information on phone numbers generated by a pen register should substantially reduce the need for NSLs.]

Unclassified

## Part 3

### ■ Changes in National Security Letters

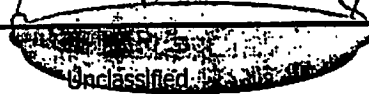




# National Security Letters

## Highlights

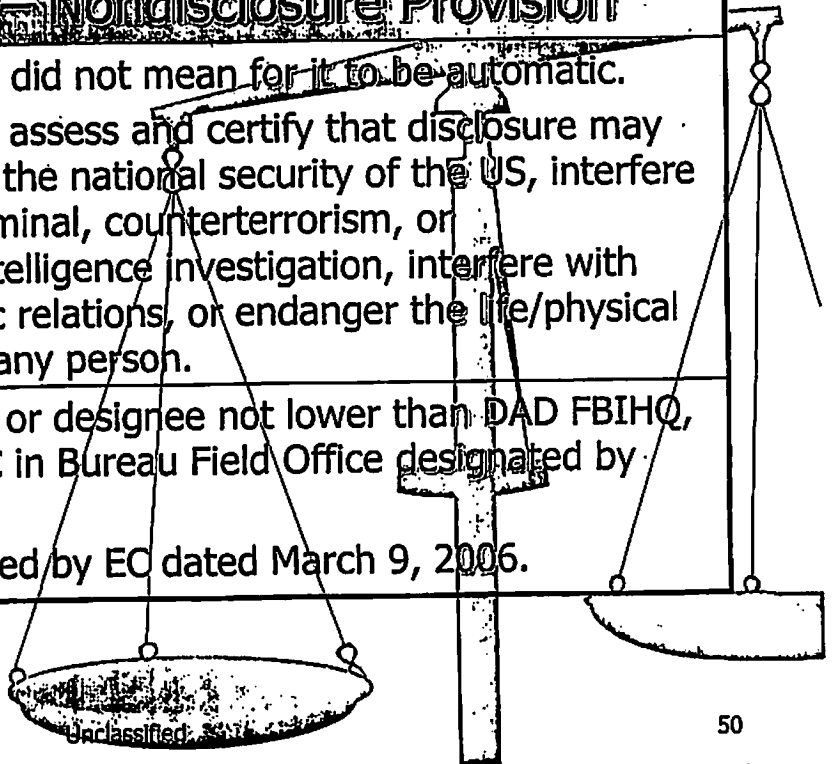
- Confidentiality – nondisclosure provision.
- Recipient challenge/Judicial review.
- Enforcement of NSLs.
- Violation of nondisclosure provision.
- Changes to Congressional reporting.



Unclassified

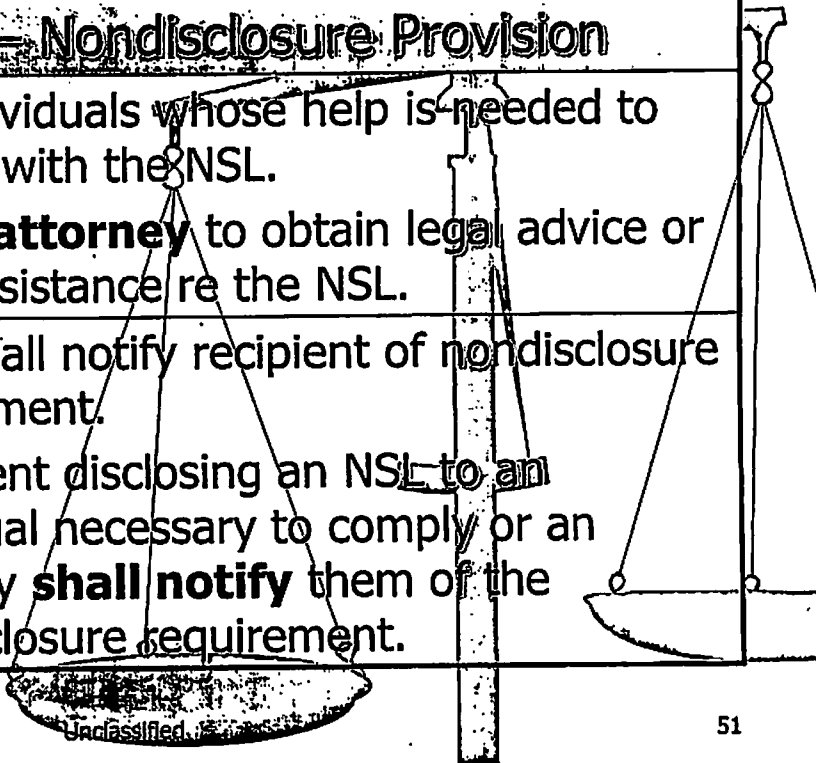
# National Security Letters

| <b>Confidentiality – Nondisclosure Provision</b> |   |
|--|---|
| <b>Activated by FBI Certification</b>            | <ul style="list-style-type: none"><li>▪Congress did not mean for it to be automatic.</li><li>▪FBI must assess and certify that disclosure may endanger the national security of the US, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life/physical safety of any person.</li></ul> |
| <b>Authority Level</b>                           | <ul style="list-style-type: none"><li>▪Director, or designee not lower than DAD FBIHQ, or an SAC in Bureau Field Office designated by Director.</li><li>▪Designated by EO dated March 9, 2006.</li></ul>  |



# National Security Letters

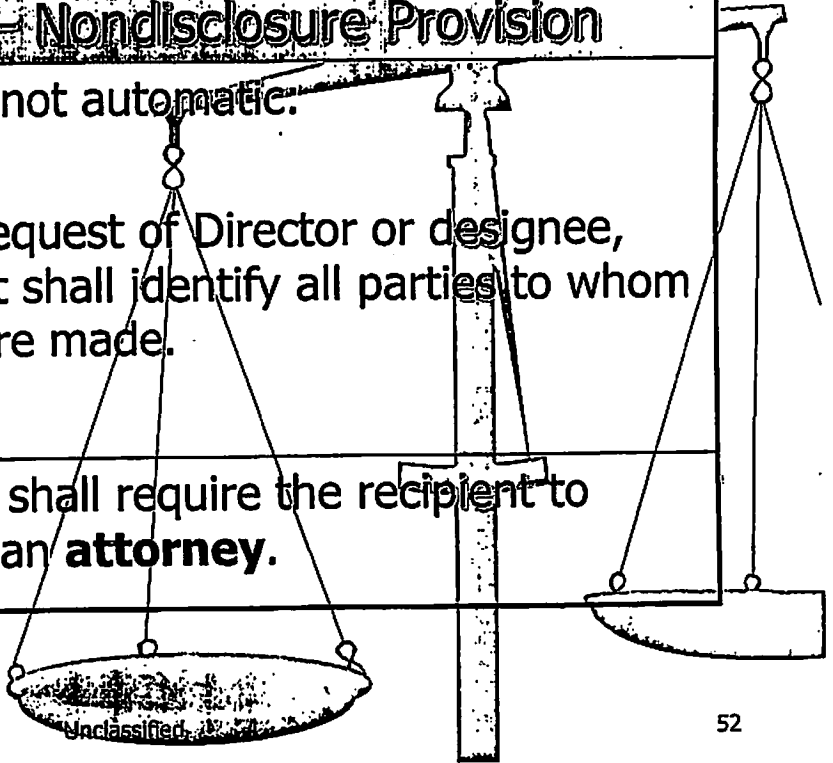
| Confidentiality – Nondisclosure Provision |   |
|---|---|
| Permitted Disclosure by Recipient         | <ul style="list-style-type: none"><li>▪ To individuals whose help is needed to comply with the NSL.</li><li>▪ To an <b>attorney</b> to obtain legal advice or legal assistance re the NSL.</li></ul>  |
| Notice                                    | <ul style="list-style-type: none"><li>▪ NSL shall notify recipient of nondisclosure requirement.</li><li>▪ Recipient disclosing an NSL to an individual necessary to comply or an attorney <b>shall notify</b> them of the nondisclosure requirement.</li></ul> |



Unclassified

# National Security Letters

| Confidentiality – Nondisclosure Provision                         |   |
|---|---|
| FBI request for Identification of parties to whom disclosure made | Again – not automatic.<br><br>At the request of Director or designee, recipient shall identify all parties to whom disclosure made. |
| <b>EXCEPT</b>   | Nothing shall require the recipient to identify an <b>attorney</b> .  |



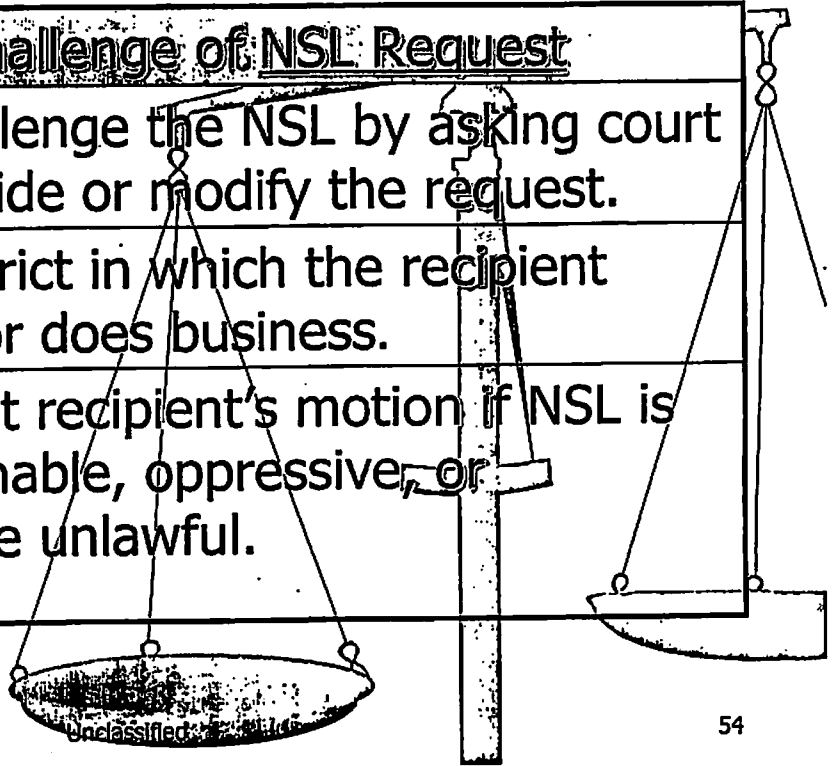
# National Security Letters

| <b>Confidentiality - Libraries</b>  |  |
|-------------------------------------|--|
| 18 USC 2709<br>No NSL in most cases | Library services - including Internet access, books, journals, magazines, newspapers, or other similar forms of printed or digital communication - do not make a library a wire/electronic communications provider for NSL purposes. |
| May serve an NSL if --              | Library is providing "electronic communication service" as defined in 18 USC 2510(15).<br>[May need to get additional information to determine if library meets the definition.]   |

Unclassified

# National Security Letters

| Recipient's Challenge of NSL Request |  |
|--------------------------------------|--|
| Recipient                            | May challenge the NSL by asking court to set aside or modify the request.                |
| Jurisdiction                         | U.S. District in which the recipient resides or does business.                           |
| Court                                | Will grant recipient's motion if NSL is unreasonable, oppressive, or otherwise unlawful. |



Unclassified

# National Security Letters

## Recipient's Challenge of NSL Nondisclosure (within one year of NSL)

|              |  |
|--------------|--|
| Jurisdiction | US District in which recipient resides or does business.   |
| Court        | May modify/set aside the nondisclosure provision if no reason to believe that disclosure may— <ul style="list-style-type: none"><li>▪ endanger the national security of the US;</li><li>▪ interfere with criminal, counterterrorism, or counterintelligence investigation;</li><li>▪ interfere with diplomatic relations; or</li><li>▪ endanger the life or physical safety of any person.</li></ul> |

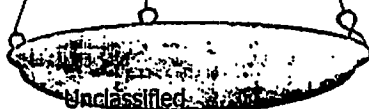
Unclassified

# National Security Letters

## Recipient's Challenge of NSL Nondisclosure (within one year of NSL)

Conclusive  
Certification

- Authority level: AG, DAG, an Assistant AG, or the Director of the FBI.
- Court will treat as conclusive the certification that disclosure may endanger the national security of the US or interfere with diplomatic relations (unless the court determines it was made in bad faith).



Unclassified



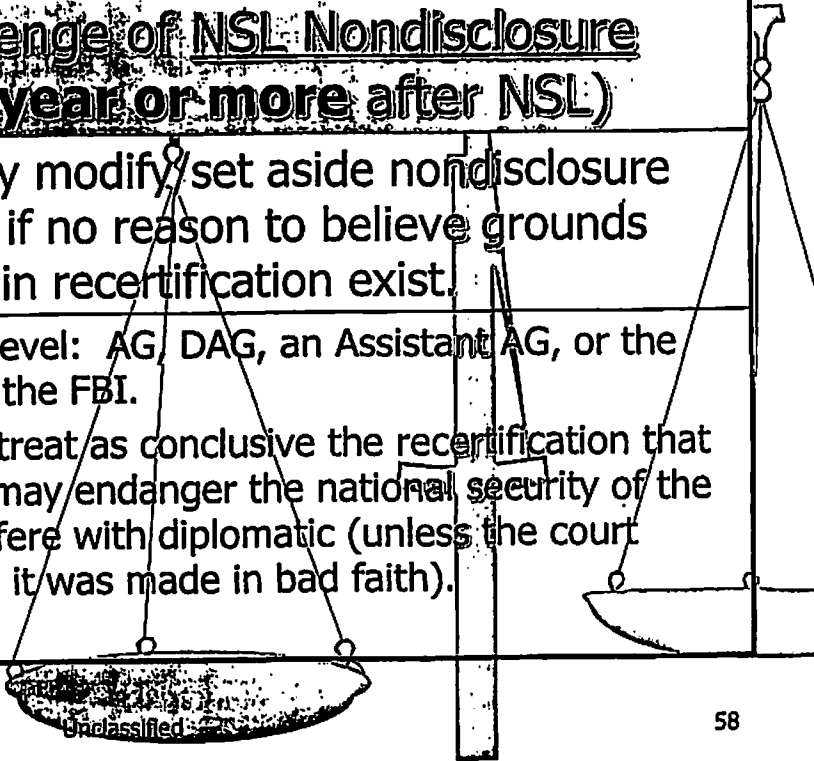
# National Security Letters

| <u>Recipient's Challenge of NSL Nondisclosure Provision (one year or more after NSL)</u> |   |
|--|---|
| Jurisdiction   | US District in which recipient resides or does business.  |
| Government   | Within 90 days of petition, the AG, DAG, an AAG, Director, or his designee in a position not lower than DAD at FBIHQ or an SAC in FBI Field Office either terminate or recertify that the disclosure may -- <ul style="list-style-type: none"><li>•endanger the national security of the US;</li><li>•interfere with criminal, counterterrorism or counterintelligence investigation;</li><li>•interfere with diplomatic relations; or</li><li>•endanger the life or physical safety of any person.</li></ul> |

Unclassified

# National Security Letters

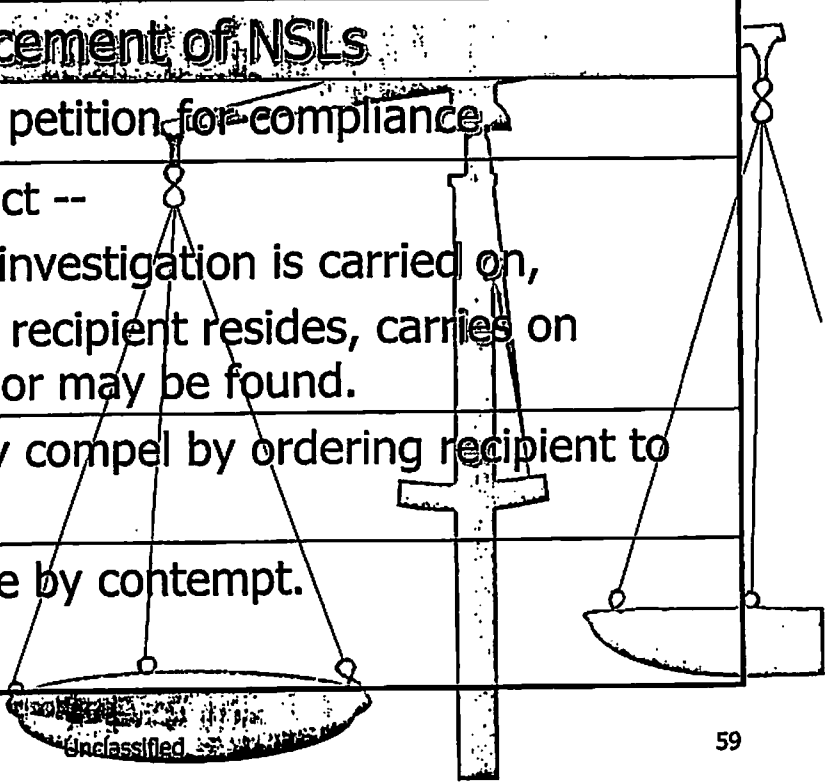
| <u>Recipient's Challenge of NSL Nondisclosure Provision (one year or more after NSL)</u> |   |
|--|---|
| Court  | Court may modify/set aside nondisclosure provision if no reason to believe grounds specified in recertification exist.  |
| Conclusive Recertification   | <ul style="list-style-type: none"><li>• Authority level: AG, DAG, an Assistant AG, or the Director of the FBI.</li><li>• Court will treat as conclusive the recertification that disclosure may endanger the national security of the US or interfere with diplomatic (unless the court determines it was made in bad faith).</li></ul> |



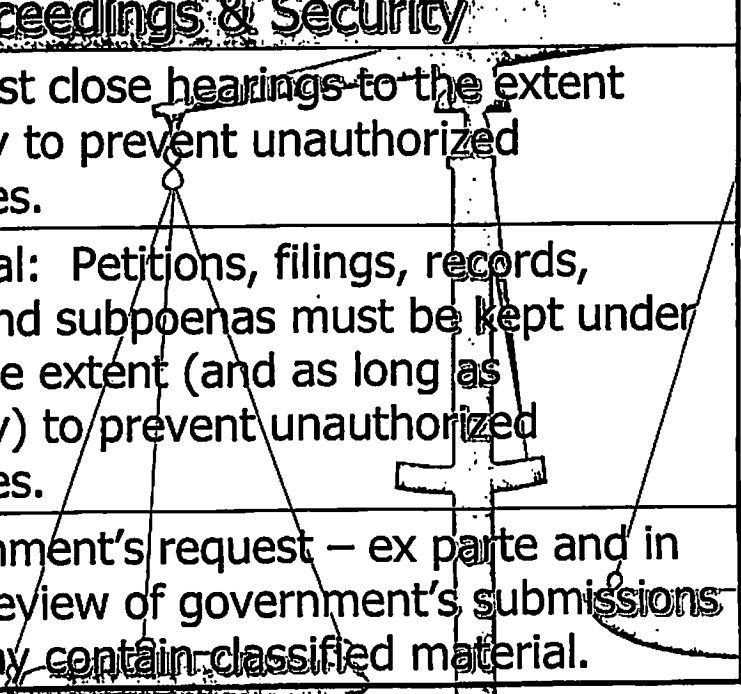
Unclassified

# National Security Letters

| Enforcement of NSLs |  |
|---------------------|--|
| Government          | May file a petition for compliance.  |
| Jurisdiction        | U.S. District --<br>▪ in which investigation is carried on,<br>▪ or where recipient resides, carries on business, or may be found. |
| Court               | Court may compel by ordering recipient to comply.  |
| Failure to Comply   | Punishable by contempt.  |



# National Security Letters



| Court Proceedings & Security |  |
|------------------------------|--|
| Hearings                     | Court must close hearings to the extent necessary to prevent unauthorized disclosures.   |
| Documents                    | Under seal: Petitions, filings, records, orders, and subpoenas must be kept under seal to the extent (and as long as necessary) to prevent unauthorized disclosures. |
| Ex Parte                     | At government's request – ex parte and in camera review of government's submissions which may contain classified material.   |

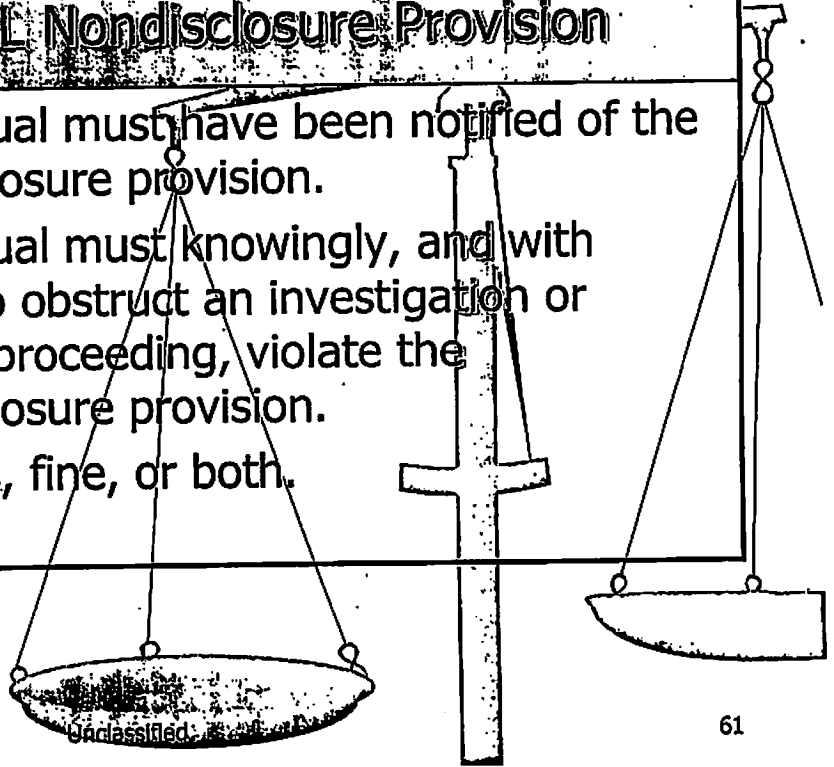
Unclassified

# National Security Letters

## Violations of NSL Nondisclosure Provision

Obstruction of  
an  
Investigation  
18 USC 1510

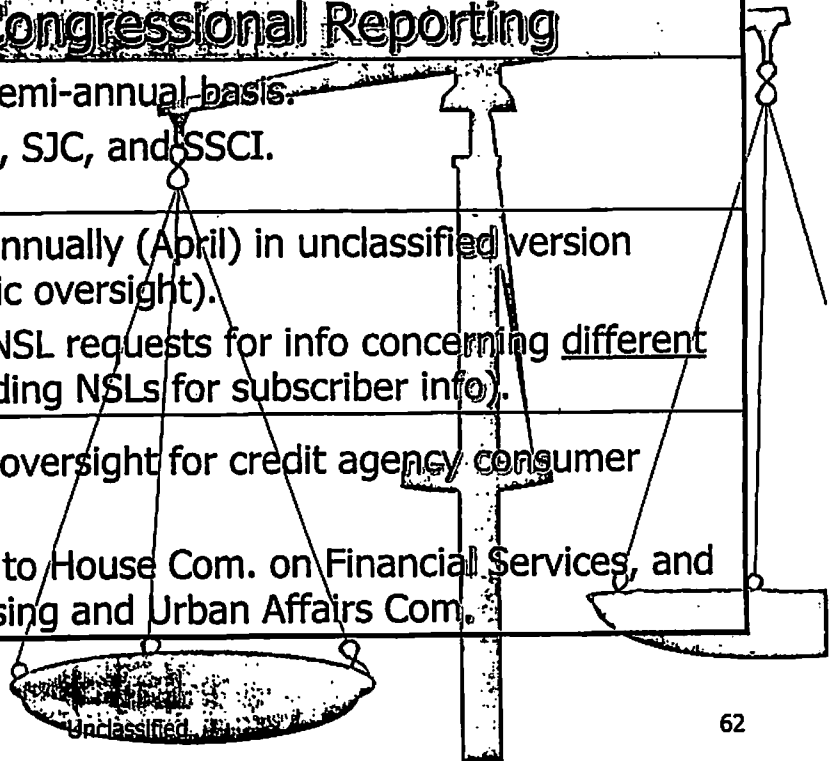
- Individual must have been notified of the nondisclosure provision.
- Individual must knowingly, and with intent to obstruct an investigation or judicial proceeding, violate the nondisclosure provision.
- 5 years, fine, or both.



Unclassified

# National Security Letters

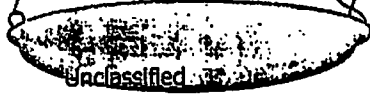
| Oversight - Congressional Reporting |  |
|-------------------------------------|--|
| NSL reports<br>Classified           | <ul style="list-style-type: none"> <li>•AG report semi-annual basis.</li> <li>•HJC, HPSCI, SJC, and SSCI.</li> </ul>   |
| Aggregate<br>NSLs<br>Unclassified   | <ul style="list-style-type: none"> <li>•AG report annually (April) in unclassified version (allows public oversight).</li> <li>•Total # of NSL requests for info concerning <u>different</u> USPs (excluding NSLs for subscriber info).</li> </ul> |
| 15 USC 1681v<br>NSLs                | <ul style="list-style-type: none"> <li>•Enhanced oversight for credit agency consumer records.</li> <li>•Also report to House Com. on Financial Services, and Senate Housing and Urban Affairs Com.</li> </ul>                                     |



Unclassified

# National Security Letters

| DOJ IG Comprehensive Audit of NSLs |  |
|------------------------------------|--|
| Scope                              | Comprehensive audit of the use of NSLs:<br>-including noteworthy facts/circumstances; and<br>-including any improper or illegal use.                   |
| Timing                             | ▪2003 - 2004 (March 9, 2007)<br>▪2005 - 2006 (December 31, 2007)   |
| Report to                          | House Judiciary Committee<br>House Permanent Select Committee on Intelligence<br>Senate Judiciary Committee<br>Senate Select Committee on Intelligence |



# National Security Letters

## DOJ IG Comprehensive Audit of NSLs

Examine effectiveness of NSLs

- Importance of the info acquired by NSLs to DOJ's intelligence activities and to the IC.
- How info is collected, retained, analyzed, and disseminated (including raw data) to member of the IC, and other federal, state, local, or tribal governments, or private sector entities.
- How often NSL info was used to produce an analytical intelligence product for distribution.

Unclassified



# National Security Letters

## DOJ IG Comprehensive Audit of NSLs

Examine  
the process

- Whether/how often NSL info was provided to law enforcement for use in criminal investigations.
- # of NSLs issued without the certification necessary to create a nondisclosure obligation.
- Types of electronic communications and transactional info obtained under sec. 2709, and the procedures DOJ used if content was obtained.



Unclassified

# National Security Letters

## DOJ IG Comprehensive Audit of NSLs

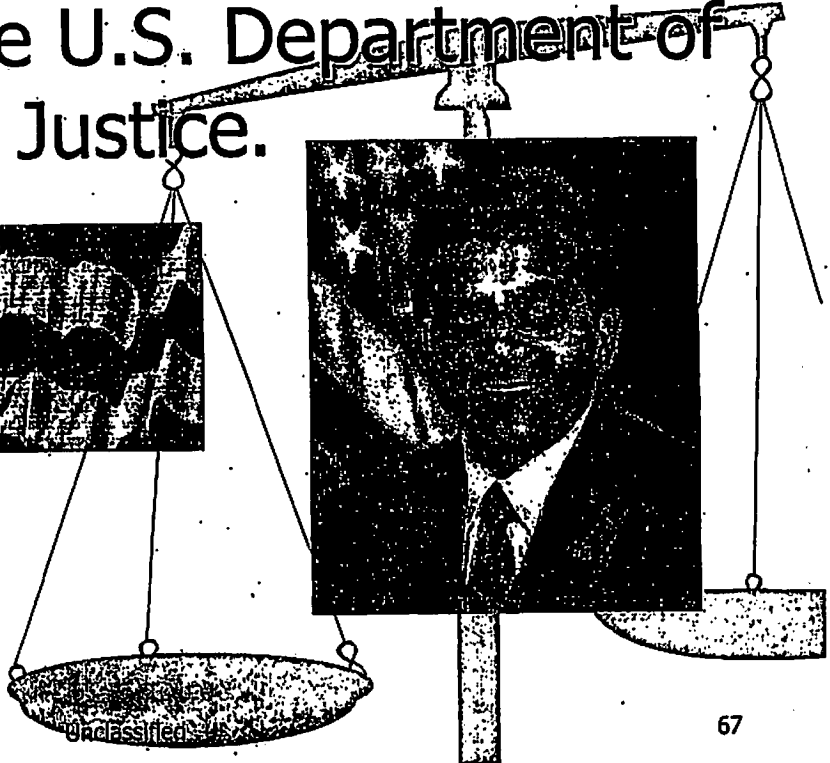
Feasibility of  
Minimization  
Procedures

- The AG and the DNI shall submit a report to Congress on the feasibility of applying minimization procedures to NSLs to ensure the protection the constitutional rights of US Persons.
- February 1, 2007 (or upon completion of 2003/2004 audit).

Unclassified

# Part 4

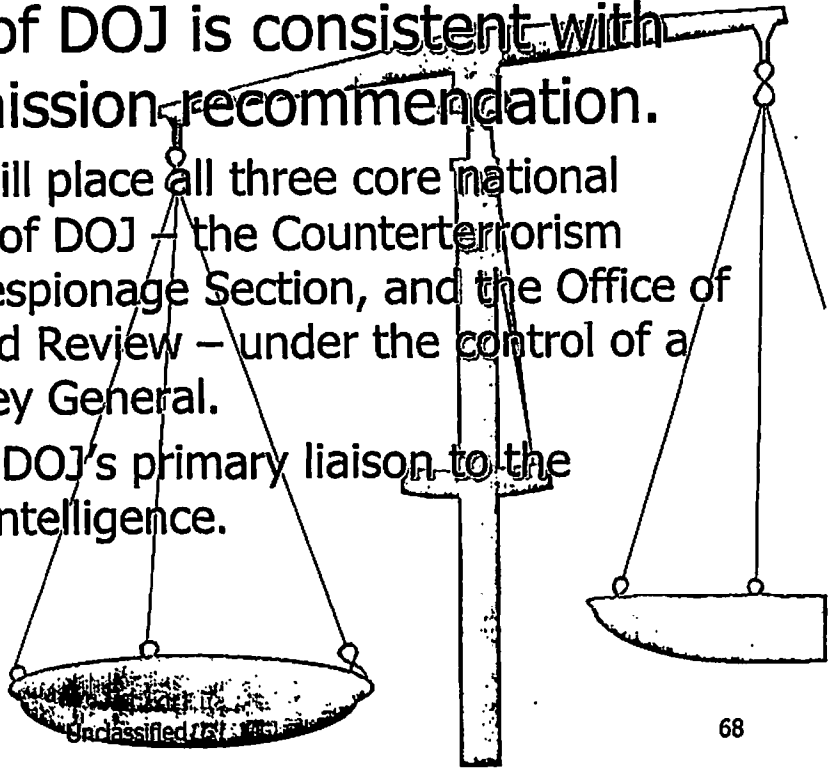
## Changes at the U.S. Department of Justice.



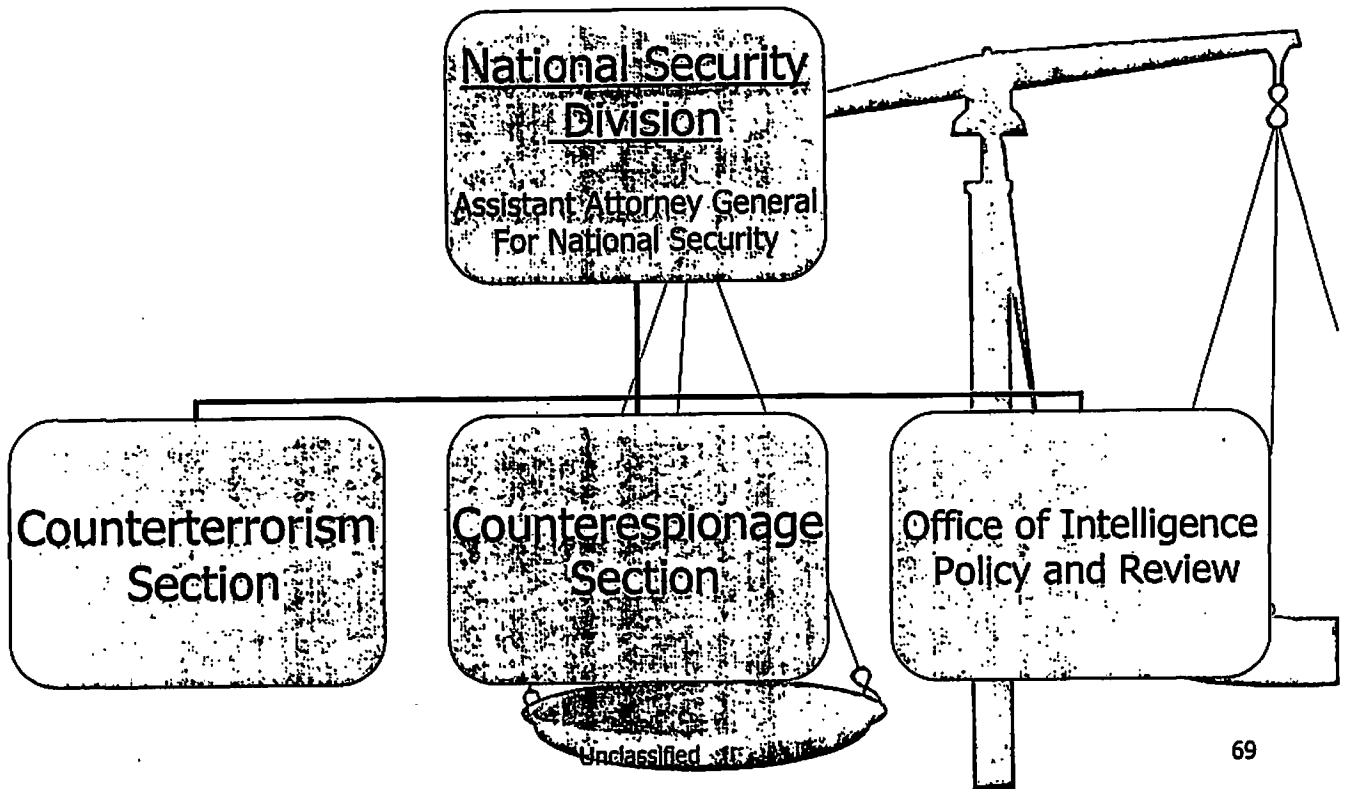
Unclassified

# U.S. Department of Justice

- Reorganization of DOJ is consistent with the WMD Commission recommendation.
- This reorganization 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 will be DOJ's primary liaison to the Director of National Intelligence.

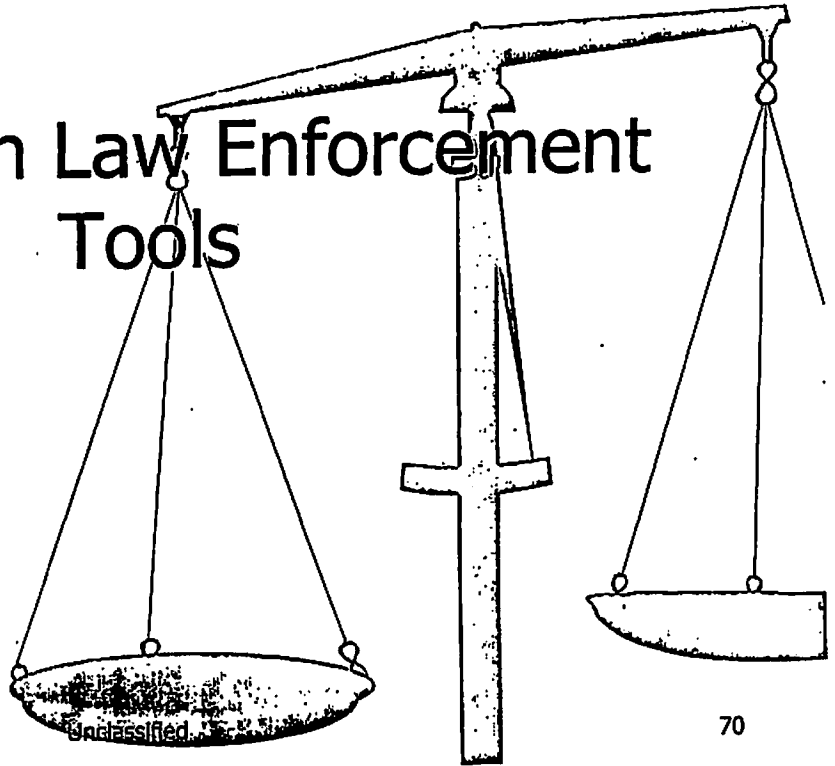


# U.S. Department of Justice



# Part 5

## ■ Changes in Law Enforcement Tools

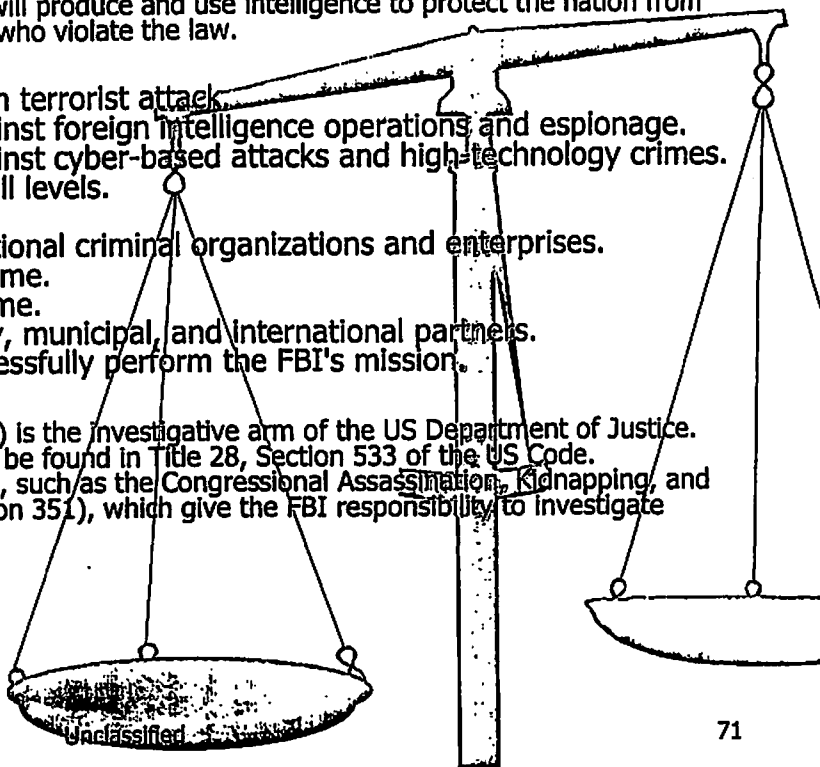


# FBI Priorities

In executing the following priorities, we will produce and use intelligence to protect the nation from threats and to bring to justice those who violate the law.

1. Protect the United States from terrorist attack.
2. Protect the United States against foreign intelligence operations and espionage.
3. Protect the United States against cyber-based attacks and high-technology crimes.
4. Combat public corruption at all levels.
5. Protect civil rights.
6. Combat transnational and national criminal organizations and enterprises.
7. Combat major white-collar crime.
8. Combat significant violent crime.
9. Support federal, state, county, municipal, and international partners.
10. Upgrade technology to successfully perform the FBI's mission.

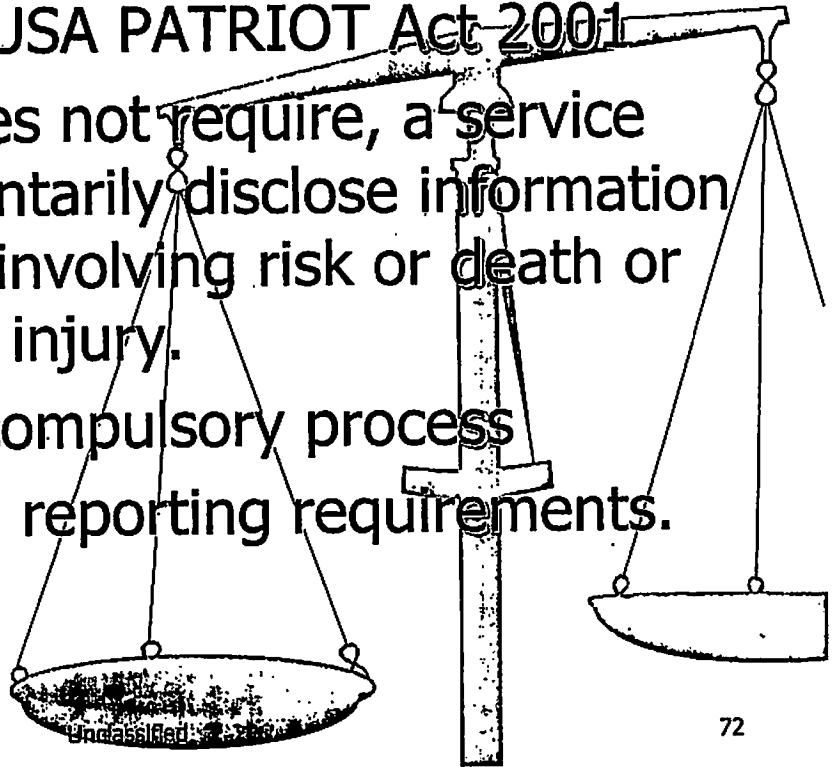
The Federal Bureau of Investigation (FBI) is the investigative arm of the US Department of Justice. The FBI's investigative authority can be found in Title 28, Section 533 of the US Code. Additionally, there are other statutes, such as the Congressional Assassination, Kidnapping, and Assault Act (Title 18, US Code, Section 351), which give the FBI responsibility to investigate specific crimes.



# 18 USC 2702

## Good Faith Emergency Disclosures

- Created by the USA PATRIOT Act 2001
- Permits, but does not require, a service provider to voluntarily disclose information in emergencies involving risk or death or serious physical injury.
- Outside of the compulsory process
- Congress added reporting requirements.





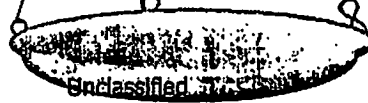
# 18 USC 2702

## Good Faith Emergency Disclosures

### Voluntary Disclosure by Service Provider

Standard remains the same:

If the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay.

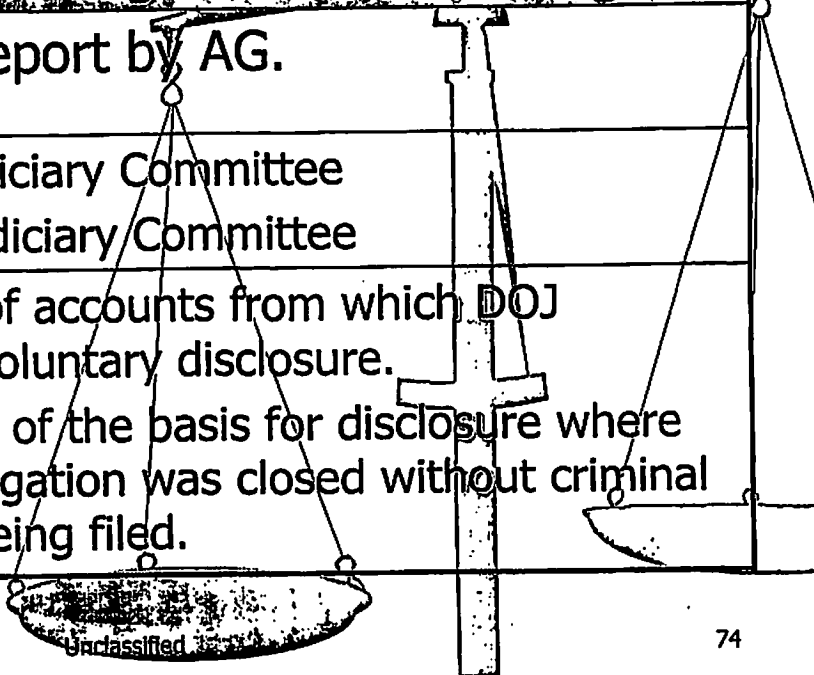


Unclassified, 17, 5

# 18 USC 2702

## Good Faith Emergency Disclosures

| Oversight – New Congressional Reporting |   |
|---|---|
| Reporting Cycle                         | Annual report by AG.  |
| Congressional Committees                | House Judiciary Committee<br>Senate Judiciary Committee   |
| Reporting Requirements                  | <ul style="list-style-type: none"><li>▪ Number of accounts from which DOJ received voluntary disclosure.</li><li>▪ Summary of the basis for disclosure where the investigation was closed without criminal charges being filed.</li></ul> |



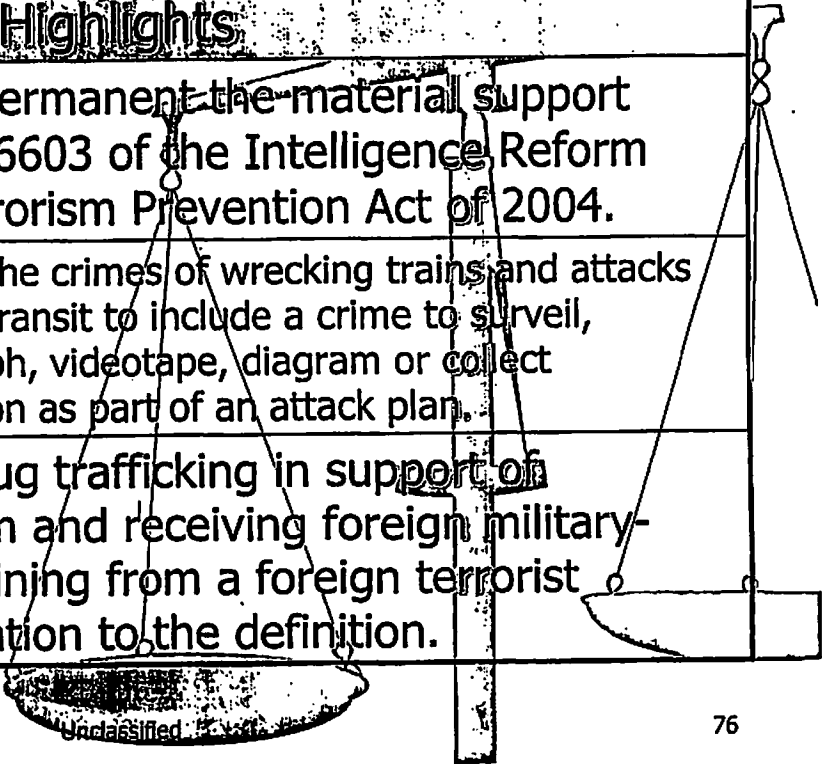
Unclassified

# 18 USC 3103a

## Delayed Notice Search Warrants

|                                      |  |
|--------------------------------------|--|
| <p><b>Notification Delay</b></p>     | <p>Presumptive – no more than <b>30 days</b> (or later date certain if facts justify).</p> <p>▪ Court may delay notice if it finds reasonable grounds to believe immediate notice may have adverse results as defined by 18 USC 2705 [endangering individual's life/physical safety, flight from prosecution, destruction of evidence, intimidation of witnesses, seriously jeopardizing investigation] "except if the adverse results consist only of unduly delaying a trial."</p> |
| <p><b>Extensions</b></p>             | <p><b>90 days</b> (unless facts justify longer)</p>  |
| <p><b>Reporting Requirements</b></p> | <p>Annual reporting to Congress by Court.</p>  |

# Federal Crimes Related to Terrorism



| Highlights                 |   |
|----------------------------|---|
| Material Support           | Makes permanent the material support Section 6603 of the Intelligence Reform and Terrorism Prevention Act of 2004.  |
| Mass Transportation        | Expands the crimes of wrecking trains and attacks on mass transit to include a crime to surveil, photograph, videotape, diagram or collect information as part of an attack plan. |
| Federal Crime of Terrorism | Adds drug trafficking in support of terrorism and receiving foreign military-type training from a foreign terrorist organization to the definition.                               |

Unclassified 3-2011

# Federal Crimes Related to Terrorism

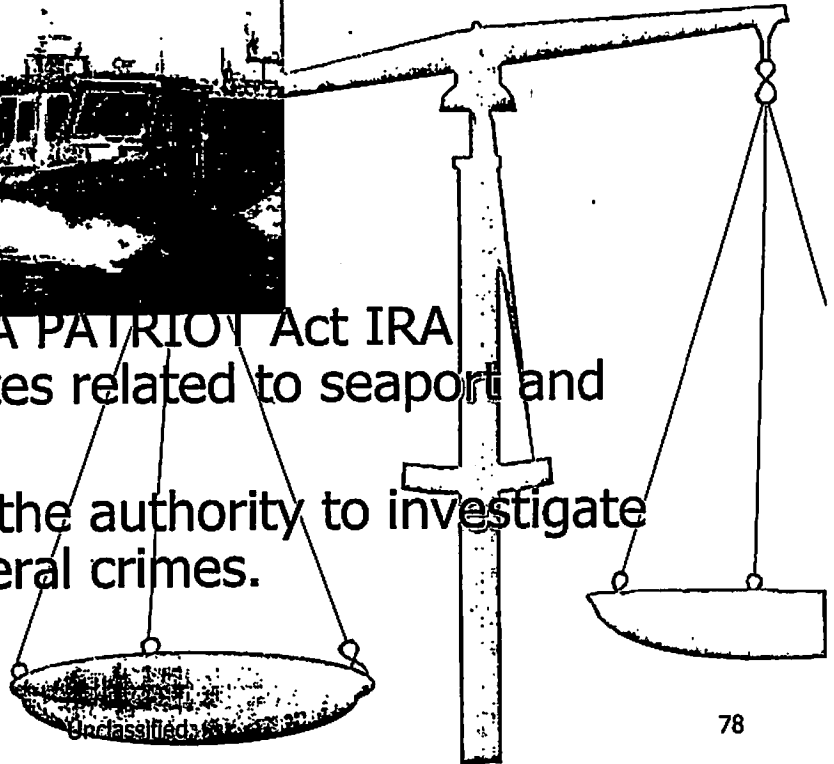
| More Highlights      |   |
|----------------------|---|
| Narco-Terrorism      | New federal crime to engage in drug trafficking to benefit terrorism.   |
| Title III Predicates | 20 federal crimes related to terrorism added to the predicate list, including: <ul style="list-style-type: none"><li>• violence at international airports;</li><li>• animal enterprise terrorism;</li><li>• biological agents;</li><li>• nuclear and weapons of mass destruction threats;</li><li>• explosive materials;</li><li>• conspiracy to harm persons or property overseas;</li><li>• attacks on mass transit;</li><li>• torture;</li><li>• harboring terrorists;</li><li>• receiving military-type training from a foreign terrorist organization; and</li><li>• structuring transactions to evade reporting requirements.</li></ul> |

Unclassified

# Reducing Crime and Terrorism at America's Seaports Act of 2005



- Title III of the USA PATRIOT Act IRA strengthens statutes related to seaport and maritime safety.
- The FBI will have the authority to investigate several of the federal crimes.



Unclassified//SI//NF

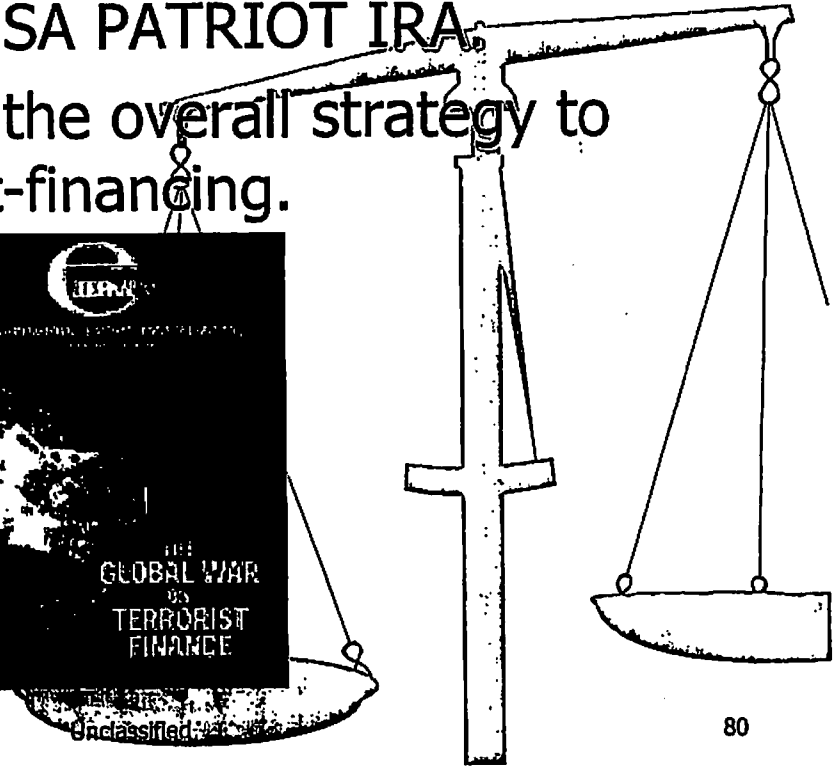
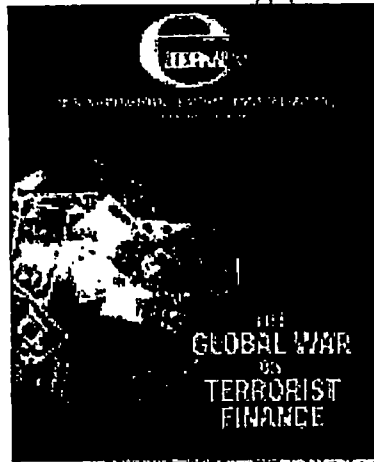
# Reducing Crime and Terrorism at America's Seaports Act of 2005

| Highlights      |   |
|-----------------|---|
| WMDs            | Federal crime to transport aboard a vessel an explosive, biological agent, chemical weapon, or radioactive or nuclear material with the intent to use it in a federal crime of terrorism. |
| Terrorists      | Prohibits the maritime transportation of terrorists.  |
| Bribery         | Federal crime to give/take bribe with the intent to commit international or domestic terrorism affecting port security.   |
| Smuggling Goods | New federal crime for illegally smuggling goods from the United States.   |

Unclassified

# Combating Terrorism Financing Act of 2005

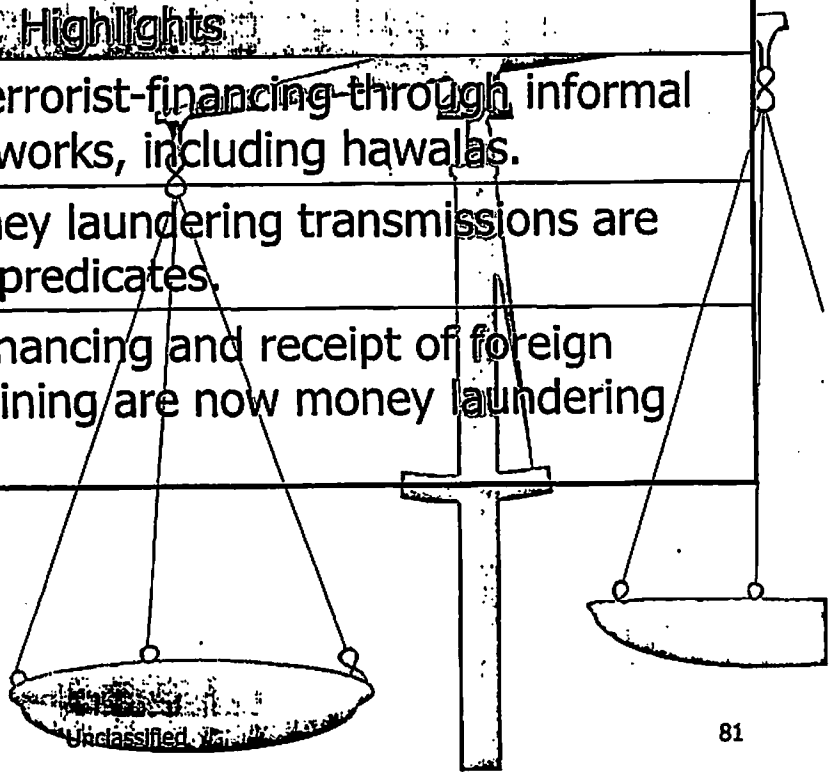
- Title IV of the USA PATRIOT IRA
- Carries forward the overall strategy to combat terrorist-financing.





# Combating Terrorism Financing Act of 2005

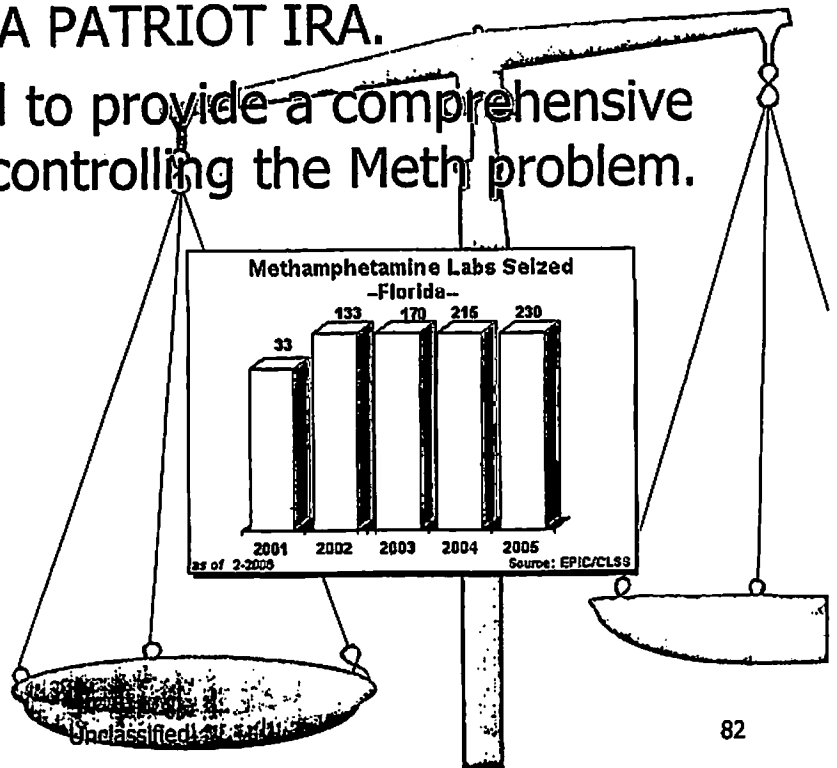
| Highlights                      |   |
|---------------------------------|---|
| Hawalas                         | Prohibits terrorist-financing through informal money networks, including hawalas.                 |
| New RICO Predicates             | Illegal money laundering transmissions are now RICO predicates.                                   |
| New Money Laundering Predicates | Terrorist-financing and receipt of foreign military training are now money laundering predicates. |



Unclassified

# Combat Methamphetamine Epidemic Act of 2005

- Title VII of the USA PATRIOT IRA.
- Congress intended to provide a comprehensive approach toward controlling the Meth problem.

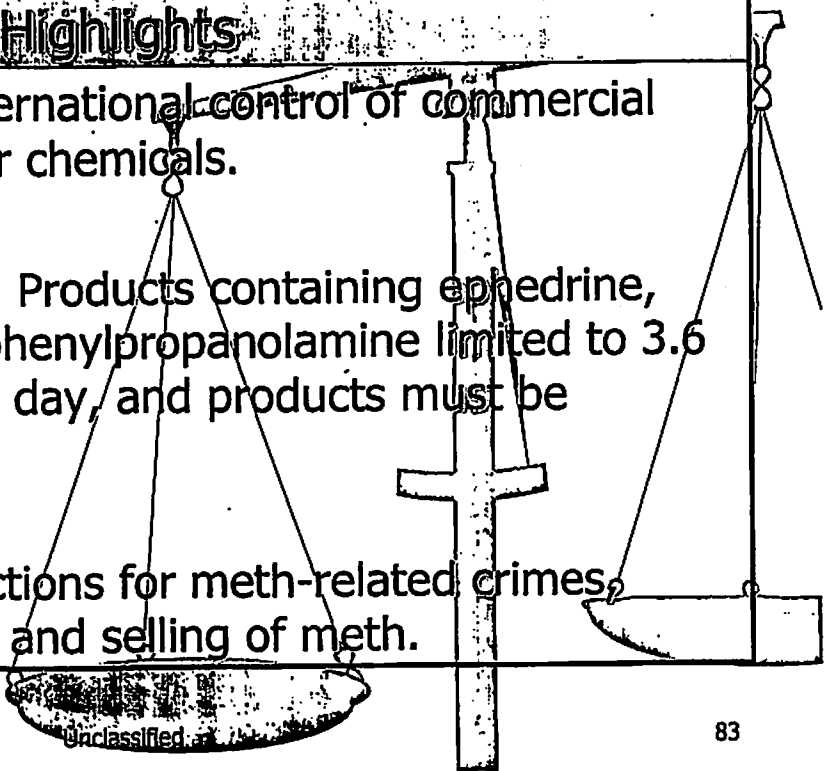


Unclassified

# Combat Methamphetamine Epidemic Act of 2005.

## Highlights

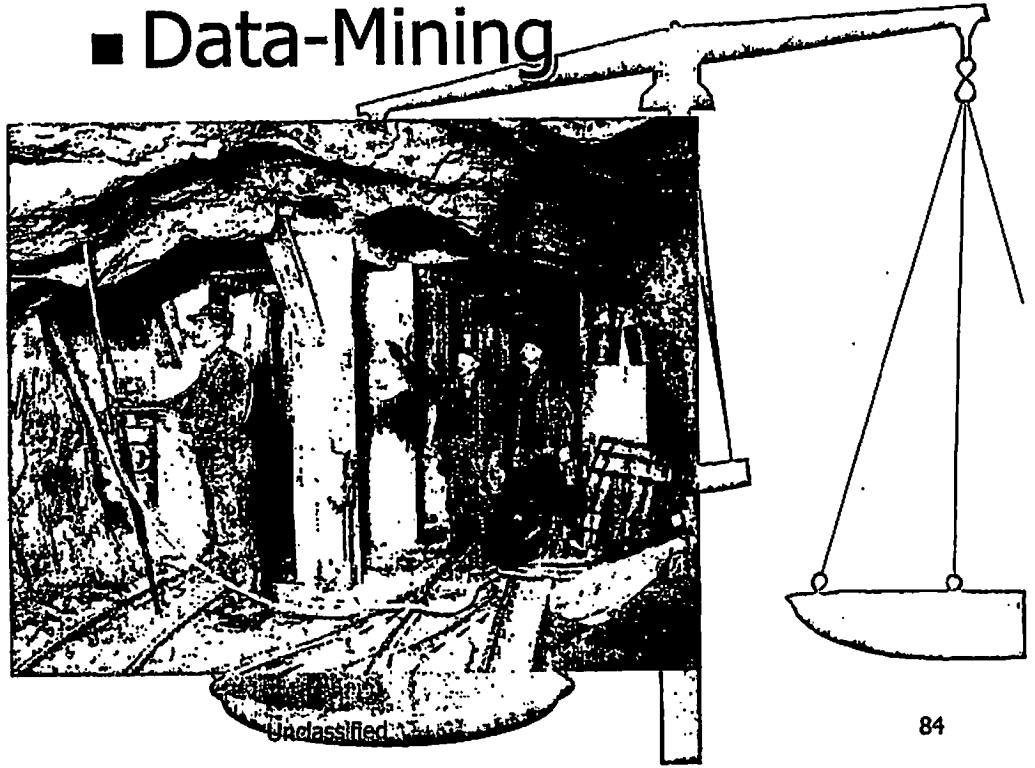
- Increased domestic/international control of commercial transactions in precursor chemicals.
- Retail/pharmacy sales: Products containing ephedrine, pseudoephedrine, and phenylpropanolamine limited to 3.6 grams per customer per day, and products must be "behind the counter."
- Enhanced criminal sanctions for meth-related crimes, including the smuggling and selling of meth.



Unclassified

# Part 6

## ■ Data-Mining

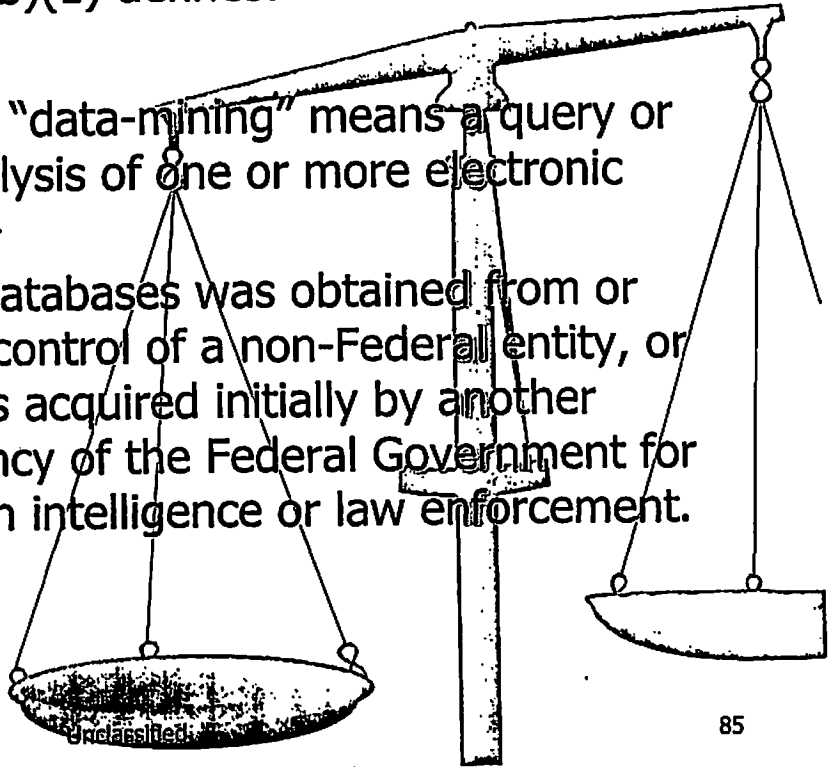


# Data-Mining

USAPA IRA section 126(b)(1) defines:

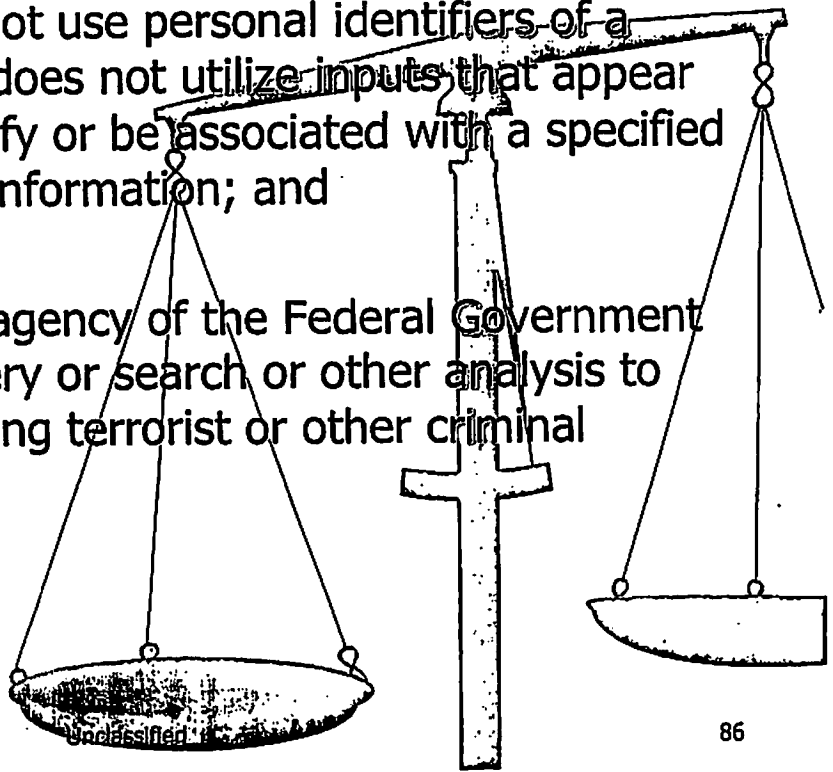
**Data-Mining.**—The term “data-mining” means a query or search or other analysis of one or more electronic databases, where—

- (A) at least one of the databases was obtained from or remains under the control of a non-Federal entity, or the information was acquired initially by another department or agency of the Federal Government for purposes other than intelligence or law enforcement.



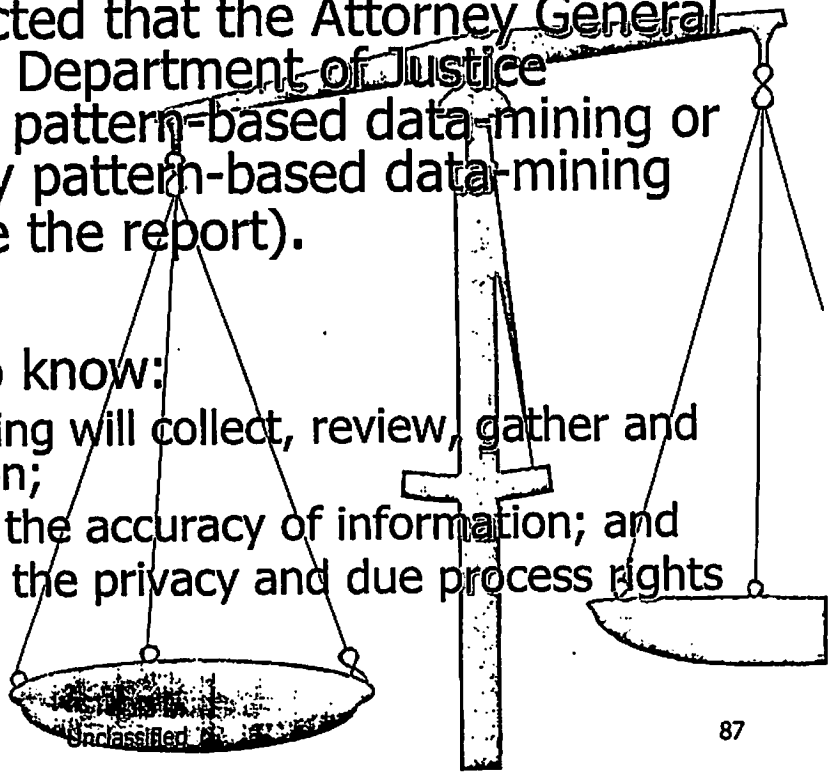
# Data-Mining

- (B) the search does not use personal identifiers of a specific individual or does not utilize inputs that appear on their face to identify or be associated with a specified individual to acquire information; and
- (C) a department or agency of the Federal Government is conducting the query or search or other analysis to find a pattern indicating terrorist or other criminal activity.



# Data-Mining

- Congress has directed that the Attorney General report on any U.S. Department of Justice initiatives that use pattern-based data-mining or are developing any pattern-based data-mining (FBI will help write the report).
- Congress wants to know:
  - How the data-mining will collect, review, gather and analyze information;
  - How it will ensure the accuracy of information; and
  - How it will protect the privacy and due process rights of individuals.

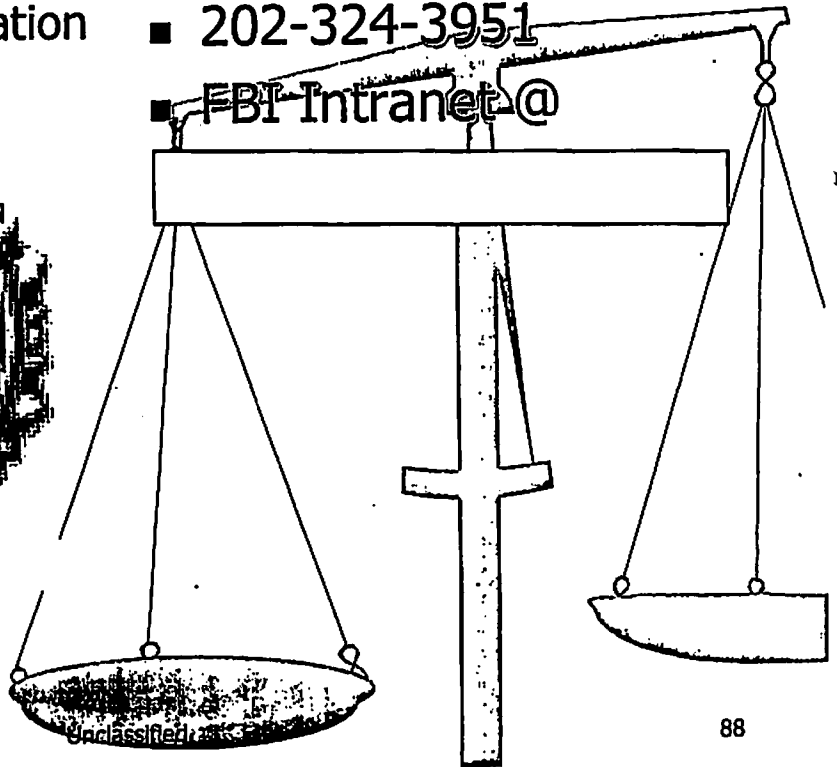
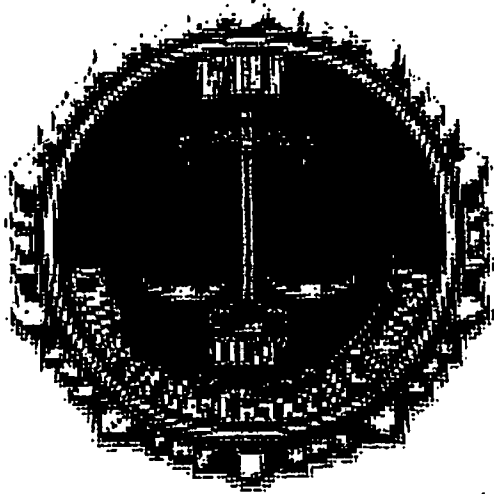


# National Security Law Branch

■ For additional information

■ 202-324-3951

■ [FBI Intranet](#)@



b7E

Unclassified//~~LES~~



# The End

This has been a production of the National Security Law Training and Policy Unit.

