



---

# ***Procedure 5***

# ***Electronic Surveillance***



# Agenda

---

- **Key changes to Procedure 5**
- **Why changes were made**
- **Review of Procedure 5**



# Procedure on Electronic Surveillance

---

This procedure applies to electronic surveillance conducted in accordance with Procedures 1, 2, 3, and 4.



# What's Different?

---

- **Statutory changes**
- User friendly
  - Try not to restate text of the statute if possible
  - Aim to identify “big rocks” for operators
  - Facilitate training
  - Remain technology neutral
  - Use concise, clear, and comprehensible language
- Guide – not a FISA practitioner’s handbook
- Public concerns/optics



# Where did we come from?

---

## 1982

- Michael Jackson releases “Thriller Album” which became the biggest selling album of all time
- EPCOT Theme Park opens at Disney
- Sony launches first consumer compact disc player
- Born - Prince William, Jessica Biel, Anne Hathaway, Apolo Ohno
- Music
  - “Eye of the Tiger,” “Let’s Get Physical,” “Ebony and Ivory,” “Gloria,” “Who Can It Be Now,” “Gloria,” and NSA’s favorite “Eye in the Sky”
- TV – “Cheers,” “Knight Rider,” “Fame,” “Family Ties”
- Movies – *E.T.*, *An Officer and a Gentleman*, *Tootsie*, *Poltergeist*
- Postage Stamp \$.20, Gas \$1.19, Bread \$.60, New Home \$83,900
- News – John Hinckley not guilty by reason of insanity for shooting President Reagan; Argentina invades Falkland Islands, Princess Grace (age 52) dies after car goes off mountain road



# Where did we come from? (cont.)

---

## 1974

- Seymour Hersh authors NY Times article “Huge CIA Operation Reported in U.S. Against Anti-War Forces”

## 1975

- **Church and Pike Committees**
  - Surveillance of journalists, including wiretapping
  - Covert mail opening
  - Plots to assassinate foreign leaders
  - Surveillance of private citizens due to anti-war activities
  - Files kept on Americans considered anti-war activists
  - Army conducting domestic surveillance of political activists
- **Legislation**
  - Privacy Act, Foreign Intelligence Surveillance Act, Classified Information Protection Act, Intelligence Oversight Act



# Foreign Intelligence Surveillance Act (FISA)

---

## 1978 (basis for 1982 DoD 5240.1-R, Procedure 5)

- Provides a statutory framework for conducting (as part of an investigation to gather foreign intelligence information) electronic surveillance and other activities to which the Fourth Amendment warrant requirement would apply if they were conducted as part of a domestic criminal investigation.
- Differences:
  - Distinct from criminal warrants;
  - Purpose is to collect foreign intelligence information; and
  - Requires probable cause to believe the person targeted is a foreign power or its agent.



# Executive Order 12333

---

Under EO 12333 the IC shall:

- Collect and provide info to policy makers and
- Collect information concerning and protecting against international terrorism, weapons of mass destruction, intelligence activities directed against the USA, international criminal drug activities, and other hostile activities by foreign powers, organizations, persons, and their agents

Foreign Intelligence means info relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists





# December 1982 DoD 5240.1-R

---

Collection of Intelligence: necessary for conduct and function of the component and falls within Procedure 2 category

## ***Procedure 5***

### **Electronic Surveillance in the U.S. for Intelligence Purposes**

- Electronic Surveillance pursuant to the Foreign Intelligence Surveillance Act
- Authority to Request Electronic Surveillance:
  - SecDef, DepSecDef, Secretary or Under Secretary of a Military Department, and DIRNSA/CHCSS
- Applications for court orders made through the AG after clearance by DoD/GC

### **Electronic Surveillance in Emergency Situations**

- Inside the United States
  - AG approval required
  - DIC may request DoD/GC seek authority from AG



# DoD 5240.1-R (cont.)

---

## **Electronic Surveillance Outside the United States for Intelligence Purposes**

- U.S. persons abroad with a reasonable expectation of privacy
- Specifically *doesn't apply to "other than U.S. persons" abroad*
- Electronic Surveillance OUTSIDE the US means the person targeted is physically outside the United States
- Need AG Approval

## **Signals Intelligence Activities**

- Collection of Foreign Communications and Military Tactical Communications
- Classified Annex to supplement

## **Technical Surveillance Countermeasures**

## **Developing, Testing, and Calibration of Electronic Equipment**

## **Training**

## **Conduct of Vulnerability and Hearability Surveys**



# Key Legislative Changes

---

## Electronic surveillance has evolved through statutory action since 1982

- Patriot Act - Roving surveillance, foreign intelligence is significant reason vice “the” reason, authorized pen/trap/trace for email, extends timeframe that authority could be granted, Section 215 - business records (bulk collection), etc.
- Intelligence Reform and Terrorism Prevention Act - “Lone Wolf” provision which obviates any need for an evidentiary connection between a person and a foreign government or terrorist group
- Protect America Act – Court orders for foreign communications of targets outside the U.S. eliminated
- FISA Amendments Act – Created Title VII, added separate procedures for targeting non-US persons and USPs reasonably believed to be outside the USA
- USA Freedom Act – Prohibited use of Sec 215 without a “selector” term (ending bulk collection)



# Overview of New Procedure 5

---

- **Basics**
- **FISA**
  - Targeting a Person in the United States
  - Targeting a US Person Outside the United States
  - Targeting a Non-USP Outside the United States
- **EO 12333**
- **Emergency Situations**
  - FISA
  - EO 12333
- **Exigent Circumstances Involving a USP Outside the United States**
- **Special Provisions**



# New Procedure 5 in Detail

---

## **Applicability**

- Implements FISA and EO 12333 requirements for conducting Electronic Surveillance
- Dependent on Mission, USP status/location, methods used, and type of communications sought
- All Electronic Surveillance must comply with Procedures 1-4

## **Need for Guidance**

- Authorities are complex – talk to your legal counsel

## **Other Legal Authorities**

- 50 USC 1841-1846 (Pen Register and Trace Devices)
- 18 USC 3121-3127 (More Pen Register and Trace Devices)
- 18 USC 2510-2522 (Electronic Communications Privacy Act)

## **Definitions**

## **Compliance with the Fourth Amendment**



# Targeting a Person in the United States

---

## Procedures

- Only the AG or FISC Judge may authorize in the USA
- DIC must comply with FISA and may only conduct if:
  - A significant purpose is to obtain FI info and
  - There is probable cause to believe target is a foreign power or an agent of a foreign power

## Authority to Request Electronic Surveillance :

- SecDef, DepSecDef, **USD(I)**, Secretary or Under Secretary of the Military Departments, DIRNSA/CHCSS
- Applications must be cleared by DoD/GC to AG



# Targeting USPs Outside the United States

---

## Procedures

- Governed by FISA and EO 12333
- DIC must comply with the following—
  - Authorized by FISA or Section 2.5 of EO 12333, and
  - There must be probable cause to believe that the target is a foreign power, an agent of a foreign power or, in some circumstances, an officer or employee of a foreign power.

## Authority to Request Electronic Surveillance

- SecDef, DepSecDef, **USD(I)**, Secretary or Under Secretary of the Military Departments, DIRNSA/CHCSS
- Applications for court orders must be cleared through DoD/GC to AG, except for
  - Applications pursuant to **Sections 703, 704, 705(a)**—may be submitted after NSA OGC clearance



# Targeting a Non-USP Outside the United States

---

## Procedures

- **Title I**
  - AG or Foreign Intelligence Surveillance Court (FISC) approval of requirements
- **Section 702**
  - Obtaining FI with the assistance of an electronic communications service provider
  - Joint Certification from AG and DNI with review by the FISC
- **Authority to Request Electronic Surveillance:**
  - SecDef, DepSecDef, **USD(I)**, Secretary or Under Secretary of the Military Departments, DIRNSA/CHCSS
  - Applications cleared by DoD/GC





# EO 12333 Electronic Surveillance

---

- **Authorized FI, CI, or support to military operations purpose**
- **Conducted IAW Executive Orders, Presidential Directives, this Manual, and Classified Annex**
- **May result in incidental collection of USP communications or information**



# Emergency Situations

---

**A DIC may conduct collection in an emergency—to take advantage of time-sensitive collection or a fleeting opportunity—only as follows:**

- **Done with Approval of the AG**
- **Authority to Request:** SecDef, DepSecDef, **USD(I)**, Secretary or Under Secretary of the Military Departments, or DIRNSA/CHCSS. The head of a DIC may request DoD/GC seek authorization directly from AG (if not feasible to submit request through individuals above).
  - For DIRNSA/CHCSS, NSA OGC may request AG Approval
- **If conducting Electronic Surveillance of a non-USP overseas under FISA 702 and the target enters the United States, under very limited circumstances the head of DIC may authorize continued surveillance for up to 72 hours.**



# Exigent Circumstances

---

---

**A DIC may conduct electronic surveillance targeting a USP outside the U.S. in exigent circumstances when securing prior approval from AG is not practical under the following conditions:**

- Life or Physical Safety is reasonably believed to be in immediate danger;
- The physical security of a DoD or FEDGOV property is in immediate danger and probable cause exists to believe the targeted USP is a foreign power, agent of a foreign power, or an officer/employee of a foreign power; **OR**
- The time required would cause failure or delay in obtaining significant FI or CI, or substantial harm to national security and probable cause exists to believe that the targeted USP is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power.

## **Authority to Approve:**

- SecDef, DepSecDef, **USD(I)**, Secretary or Under Secretary of the Military Departments, DIRNSA/CHCSS, NSA Deputy Director, a single delegee of the DIRNSA/CHCSS, NSA/CSS Senior representative present, OR any flag or general officer at the overseas location in question. Such official must promptly notify DOD/GC or NSA OGC, who will in turn notify the AG as soon as possible.
- Time Limit: No longer than 72 hours without AG approval



# Special Provisions

---

## Developing, Testing, and Calibrating Equipment

- **Applicability**
- **Signals that may be used without restriction**
- **Signals that may be used with minimization procedures**
- **Signals that may only be used with restrictions to include signals requiring AG approval for more than 90 days**
  - Scope
  - Targeting
  - Retention, Use, Dissemination
    - Technical Parameters, Content for Government Signals and Citizens/Amateur Band Radio Signals, and Other Signals



# Special Provisions (cont.)

---

## Technical Surveillance Countermeasures

- **Applicability**
- **Procedures**
  - **USD(I) authorization through policy**
  - Must comport with these conditions:
    - Not reasonable to obtain consent;
    - Use is limited in extent and duration to that necessary;
    - Authorized by official in charge; and
    - Not targeted against communications of any particular person(s)
- **Retention and Dissemination**
  - If acquired in a manner that constitutes Electronic Surveillance – data may only be retained for 18 USC 119, 47 USC 605 purposes, destroyed when no longer required
  - If not Electronic Surveillance
    - Purposes IAW with Applicability section or for collection avoidance
    - Record of types of communications and info acquired as unauthorized electronic surveillance that is detected may be retained



# Special Provisions (cont.)

---

## Training

- **Applicability**
- **Training Guidance**
- **Preferred Signals for Training Purposes**
- **Use of Other Signals for Training Purposes**
  - Not targeting particular person without consent;
  - Not reasonable to obtain consent for incidental collection;
  - Not reasonable to train without conducting Electronic Surveillance;
  - Limited in extent and duration; and
  - Minimal acquisition of info is permitted for calibration purposes
- **Retention and Dissemination**



## Special Provisions (cont.)

---

### Transmission Media Surveys - Nonconsensual surveys of transmission facilities to determine vulnerabilities

- Prior written approval DIRNSA/CHCSS or delegee;
- **When practicable, collection authorized by official in charge of the facility;**
- No transmission acquired aurally except to or from USGOV entities acquired IAW approved AG procedures;
- No content may be acquired, with the exception of the content of transmissions that are directed at or that may connect to a USG entity's facilities;
- No transmission may be recorded, except as noted above; and
- No report or log may include USPI, except to identify transmission facilities that are vulnerable to surveillance by foreign powers



# Special Provisions (cont.)

---

## Radio Communication Hearability Surveys

- **Authorized by DIRNSA/CHCSS or Delegee, and**
  - **When practicable, collection authorized by official in charge of the facility**
  - **Info must be processed and stored as follows:**
    - Content may not be recorded;
    - No transmission may be de-multiplexed/demodulated for any purpose; and
    - No report or log may ID person or entity except for purpose of identifying facility
  - **Dissemination IAW Procedure 4**





# Special Provisions (cont.)

---

## Military Tactical Exercise Communications

- The US SIGINT System may collect, process, retain, and disseminate military tactical exercise communications that contain USPI only in accordance with the Classified Annex
- Avoid incidental collection not related to exercise
- Retention and Processing
- Dissemination of military tactical communications and exercise reports will be limited to those authorities and persons participating in or reviewing such exercises



# Summary

---

- **1982 to 2016—it has been a long time coming**
  - **Statutory Changes**
  - **Mission Changes**
  - **Public Optics**
  - **Technology Changes**
- **Guiding Principles**
  - **Concise, Clear, and Comprehensible Guidance**



# Procedure 5

## Electronic Surveillance

---

**Questions?**