Air Force Office of Special Investigations

Eyes of the Eagle

CI Cyber Authorities Legal Briefing

Sept 2016

U.S. AIR FORCE

Overview

- Legal Framework
- DoDM 5240.01 Overview
- Computer Trespasser Exception
- Scenarios

CI Cyber
Legal Framework

Legal Framework—The Basics

- U.S. Constitution
- U.S. Code
  - FISA
  - ECPA
  - Computer Fraud and Abuse Act
  - Computer Trespasser Exception
  - National Security Letters
- Executive Order 12333
- DoD/USAF Issuances
  - DoDM 5240.01 (Procs 1-10)
  - DoD 5240.1-R (Procs 11-15)
  - AFI 71-101 v4

Legal Framework—History

- Spying is one of the oldest professions
  - General George Washington noted during the War of Independence "it was the British spies he feared the most."

- Today's laws and policies are the direct result of unfettered intelligence collection by DoD, FBI and CIA in the 1960's and 1970's.
  - Physical surveillance of public figures involved with the anti-Vietnam war and civil rights protests, e.g., MLK
  - Mail openings
  - Break-ins of the offices, vehicles and houses of U.S. persons
  - Undisclosed participation on university campuses

Legal Framework—History

- The Church and Pike congressional committees found the IC lacked policy on how to conduct its mission in regards to U.S. persons
  - Recommended "reining" in Executive Branch powers in using intelligence elements against U.S. persons
  - Created the Permanent Select Committee on Intelligence (Senate) and the Congressional Committee on Intelligence
  - The Foreign Intelligence Surveillance Act was enacted in 1978
- Before Congress passed legislation to correct this deficiency, E.O. 11905 was signed, which was later replaced by E.O. 12333 (standing E.O. on Intelligence Oversight)

DoDM 5240.01 Overview

DoD Manual 5240.01

Procedures Governing the Conduct of DoD Intelligence Activities

Originating Component	Office of the Deputy Chief Management Officer of the Department of Defense
Effective:	Month Day, Year
Releasability:	Cleared for public release. Available on the DoD Issuances Website at http://www.dtic.mil/whs/directives
Incorporates and Cancels:	Directive-type Memorandum 08-052, "Intelligence Oversight Policy Guidance," March 20, 2008 Procedures 1-10 of DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 7, 1982
Approved by:	Loretta E. Lynch, Attorney General of the United States Ashton B. Carter, Secretary of Defense

Purpose: In accordance with the authority in DoD Directive 5240.01 and Executive Order (E.O.) 12333, this issuance:

- Establishes procedures to enable DoD to conduct authorized intelligence activities in a manner that protects the constitutional and legal rights and the privacy and civil liberties of U.S. persons. DoD authorized intelligence activities are foreign intelligence and counterintelligence (CI) activities unless otherwise specified in this issuance.
- Authorizes the Defense Intelligence Components to collect, retain, and disseminate information concerning U.S. persons in compliance with applicable laws, Executive orders, policies, and regulations.

Eyes of the Eagle

DoDM 5240.01 Overview

- Signed by SecDef and Attorney General August 2016
- Replaces Procedures 1-10 of DoD 5240.01-R (December 1982)
- Ten (10) Procedures
  - Proc 2, Collection
  - Proc 3, Retention
  - Proc 4, Dissemination
  - Proc 5, Electronic Surveillance
  - Proc 6: Concealed Monitor
  - Proc 7, Physical Search
  - Proc 8, Mail Search/Cover
  - Proc 9, Physical Surveillance
  - Proc 10, Undisclosed Participation

DoDM 5240.01, Counterintelligence

- **Defined: Information gathered and activities conducted to *identify, deceive, exploit, disrupt,* or *protect* against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.**

Procedure 2, Introduction

- **Intentional Collection of USPI: We may *intentionally* collect USPI *only* if:**
  - **the information sought is *reasonably believed* to be *necessary* for the performance of an authorized counterintelligence mission;**
  - **the USPI falls within one of the following 13 categories below; and**
  - **we use the least intrusive means.**
- **U.S. Person Information (USPI) defined: Information that is reasonably likely to identify one or more specific U.S. persons.**
- **Collection takes place upon receipt**
  - **Regardless of when you use it**
  - **Computers can collect**
  - **Intel is collected only once**
  - **May be disseminated multiple times**
  - **Encrypted data is considered collected upon receipt**

Procedure 2, Reasonable Belief

- **Defined: When the facts and circumstances are such that a reasonable person would hold the belief.**
  - **Must rest on facts and circumstances that can be articulated;**
  - **Hunches or intuitions are not sufficient; and**
  - **Can be based on experience, training, and knowledge of CI activities as applied to particular facts and circumstances.**

Procedure 2 Categories

1. Publicly Available
2. Consent
3. Foreign Intelligence (FI)
4. Counterintelligence (CI)
5. Threats to Safety
6. Protection of Sources/Methods
7. Current, Former, or Potential Sources
8. Persons in Contact With Sources or Potential Sources
9. Personnel Security
10. Physical Security
11. Communications Security
12. Overhead and Airborne Reconnaissance
13. Administrative Purposes

Procedure 2 Categories

1. **Publicly Available Information**
2. **Consent**
   - **Defined: An agreement by a person or organization to permit a Defense Intelligence Component to take particular actions affecting that person or organization.**
   - **The legal advisor [OSI/JA] will determine whether a notice or policy is adequate and lawful, before the Component takes or refrains from taking action on the basis of implied consent.**
3. **Foreign Intelligence**

Procedure 2 Categories

4. **Counterintelligence: The information is *reasonably believed* to constitute CI and the U.S. person is one of the following:**
   - (a) **An individual, organization, or group reasonably believed to be engaged in or preparing to engage in espionage, other intelligence activities, sabotage, or assassination on behalf of a *foreign* power, organization, or person, or on behalf of an agent of a *foreign* power, organization, or person;**
   - (b) **An individual, organization, or group reasonably believed to be engaged in or preparing to engage in international terrorist activities;**
   - (c) **An individual, organization, or group reasonably believed to be acting for, or in furtherance of, the goals or objectives of an international terrorist or international terrorist organization, <u>for purposes harmful to the national security of the United States</u>; or**
   - (d) **An individual, organization, or group *in contact with a person described above* for the purpose of identifying such individual, organization, or group and assessing any relationship with the person described therein.**

Procedure 2, Other

- **Special Circumstances Collection**
  - Defense Intelligence Components will consider whether collection opportunities raise special circumstances based on the volume, proportion, and sensitivity of the USPI likely to be acquired, and the intrusiveness of the methods used to collect the information.
- **Amount of Information Collected**
  - In collecting non-publicly available USPI, to the extent practicable, collect no more information than is reasonably necessary.
- **Least Intrusive Means**
  - Use the least intrusive collection techniques feasible within the United States or directed against a U.S. person abroad.
    1. Publicly available sources or with the consent of the person concerned
    2. Cooperating sources
    3. Techniques that do *not* require a judicial warrant or AG approval
    4. Techniques that do require a judicial warrant or AG approval

Procedure 3, Retention

- **Permanent Retention standard**
  - Retention is reasonably believed to be necessary for the performance of an authorized intelligence mission; and
  - The information was lawfully collected or disseminated to the Component
    - Meets one of the 13 collection categories; or
    - Is necessary to understand or assess CI, e.g., information about a U.S. person that provides important background or context for CI.

Procedure 3, Retention

- Three primary evaluation periods to determine retention of USPI
  - Promptly
  - Five (5) years
  - Twenty-five (25) years

- Intentional Collection of USPI
  - Must be evaluated promptly; and
  - If *necessary*, may retain the information for evaluation for up to 5 years, subject to extension.

Procedure 3, Retention

- **Incidental Collection of USPI**
  - Defined: collection of USPI that is not deliberately sought, but is nonetheless collected
  - *In the United States,* may retain all of the incidentally collected information for evaluation for up to 5 years, unless extended
  - *Outside the United States, may* retain all of the incidentally collected information for evaluation for up to 25 years.

- **Voluntarily Provided USPI**
  - About a U.S. person, evaluate the information promptly, up to 5 years, unless extended.
  - About a non-U.S. person, evaluation for up to 25 years.

Procedure 3, Retention

- **Unintelligible information**
  - The time periods begin when the information is processed into intelligible form
  - Includes information that a Component cannot decrypt or understand in the original format.
  - To the extent practicable, unintelligible information will be processed into an intelligible form.
  - A foreign language is considered intelligible

- **Deletion of Information.**
  - Unless the standards for permanent retention are met, must delete all USPI from the Component's automated systems of records.

Procedure 4, Dissemination

- We may disseminate USPI based upon the following criteria:
  - Any person or entity: Information is publicly available or U.S. person has consented to the dissemination.
  - Other intelligence community elements
  - Other DoD elements; federal government entities; state, local, tribal, or territorial governments: recipient is reasonably believed to have a need to receive such information for the performance of its lawful missions or functions.
  - Foreign governments or international organizations
    - Recipient is reasonably believed to have a need to receive such information for its lawful missions or functions; and
    - Disclosure is consistent with applicable international agreements and foreign disclosure policy
  - Protective Purposes: Necessary to protect the safety or security of persons or property, or to protect against or prevent a crime or threat to the national security.

Procedure 5, Electronic Surveillance

- Implements FISA and E.O. 12333
- Defined
  - The installation or use of any monitoring device in the United States where a person has a reasonable expectation of privacy, as determined by *OSI/JA*, and
  - A warrant would be required for law enforcement purposes.
- Fourth Amendment
  - All electronic surveillance must comply with the Fourth Amendment
  - *OSI/JA* will assess the reasonableness of collection, retention, and dissemination

Procedure 5, Electronic Surveillance

- In the United States
  - Attorney General or the Foreign Intelligence Surveillance Court (FISC) may authorize, except for emergency situations.
  - May only conduct such surveillance if both:
    - A *significant purpose* of the electronic surveillance is to obtain foreign intelligence information; and
    - There is probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power.

Procedure 5, Electronic Surveillance

- Outside the United States
  - U.S. person
    - Governed by FISA and E.O. 12333; or
    - Approval under exigent circumstances exception
  - Non-U.S. person: governed by Title I or Section 702
- Emergency situations: Attorney General approval
- Technical Surveillance Countermeasures (TSCM)
  - Applies to the use of electronic equipment and specialized techniques to determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance.

Procedure 6, Concealed Monitoring

- **Defined as the following:**
  - Hidden electronic, optical, or mechanical devices,
  - to monitor a particular person or a group of persons,
  - without *consent*,
  - in a surreptitious manner,
  - over a period of time, and
  - no *reasonable expectation of privacy*.
- **Examples**
  - Video monitoring or sound recording of a subject in a place where he or she has no reasonable expectation of privacy if conducted over a period of time
  - Taking one photograph of a subject would ***not*** qualify.

Procedure 6, Concealed Monitoring

- **Scope**
  - ***Any*** **person inside the United States, or**
  - **Any U.S. person outside the United States**
- **In the United States**
  - **On DoD facilities**
  - **Outside DoD facilities, after coordination with the FBI.**
- **Outside the United States**
  - **On DoD facilities**
  - **Outside DoD facilities must be coordinated with the CIA, and appropriate host country officials in accordance with any applicable SOFA or other international agreement.**

Procedure 6, Concealed Monitoring

- Approval: AFOSI/CC or delegee
- OSI/JA will determine whether the following criteria have been met:
  - There is no reasonable expectation of privacy;
  - Such monitoring is necessary to conduct an assigned CI function;
  - A trespass will not be necessary to effect the monitoring; and
  - The monitoring is not subject to Procedure 5

Procedure 7, Physical Searches

- **Scope: Applies to *nonconsensual* physical searches in the United States *and* of U.S. persons/property outside the United States.**
- **Defined: Any intrusion on a person or property that would require a *warrant* for law enforcement purposes.**
- **Does *not* include examinations of**
  - **Areas that are in plain view and visible to the unaided eye if there is no physical trespass;**
  - **Publicly available information;**
  - **Abandoned property in a public place;**
  - **Items where we have consent; and**
  - **Government property pursuant to Military Rule of Evidence 314(d)**

Procedure 7, Physical Searches

- **Active duty**
  - Approval: Attorney General or FISC
- **Other persons inside the United States**
  - We may ***NOT*** conduct searches of other persons
  - We may request the FBI to conduct such a search
- **Other U.S. persons outside the United States**
  - The search is for an authorized foreign intelligence or CI purpose;
  - The search is appropriately coordinated with the CIA; and
  - The FISC or the Attorney General has authorized the search.
  - Authority to Request
    - Does ***not*** include AFOSI/CC
    - SecDef, DSD, USD(I); SecAF; USecAF; DIRNSA/CHCSS; Director, DIA; Director, NGA; or Director, NRO

Procedure 8, Mail Searches and Cover

- **Mail Searches**
  - See Procedure 7

- **Mail cover**
  - In U.S. postal service channels, request the USPS IAW 39 CFR 233.3(e)(2)
  - In foreign postal channels, may request a mail cover for mail that is to or from a U.S. person consistent foreign law and any applicable SOFA

Procedure 9, Physical Surveillance

- Who can we surveil in the United States:
  - Military service members;
  - Present or former military or civilian employees of a DIC;
  - Present or former contractors of a DIC;
  - Present or former employees of such a contractor;
  - Applicants for such employment or contracting;
  - Non-U.S. persons; and
  - Other persons, "when detailed to the FBI or when operating under FBI authorities."

Procedure 9, Physical Surveillance

- **Scope**
  - Any person inside the United States or any U.S. person outside the United States.
  - Applies to any devices used to observe the subject of the surveillance (not Procedure 6).

- **Defined**
  - Deliberate and continuous observation of a person, and
  - Where the person has no reasonable expectation of privacy.
  - Does *not* apply to surveillance detection or counter surveillance used to detect and elude foreign physical surveillance

Procedure 9, Physical Surveillance

- **Approval and coordination**
  - **Approval: AFOSI/CC or delegee**
  - **Coordination**
    - **In the United States**
      - No coordination req'd for surveillance of active duty, on-base
      - FBI for off-base surveillance
      - FBI for surveillance on-base, non-active duty
    - **Outside the United States**
      - CIA for off-base surveillance
      - Consider with SOFA and foreign law/policy

Procedure 10, Undisclosed Participation (UDP)

- **Scope: Governs the *participation* by DICs and anyone acting on behalf of a DIC, e.g., sources, in any *organization* in the United States or any organization outside the United States that constitutes a U.S. person.**
- **Organization defined**
  - **An association of two or more individuals formed for any *lawful* purpose whose existence is formalized in some manner**
  - **Includes those that meet and communicate through the use of technologies**
- **Participation defined**
  - **When a person is tasked or asked to participate in an organization for the benefit of the DIC**
  - **Actions undertaken "for the benefit of" a DIC may include collecting information, identifying potential sources or contacts, or establishing or maintaining cover.**

Procedure 10, UDP

- Exclusions
  - Personal participation
  - Voluntarily provided information
  - Publicly available information on the Internet
    - Collection of publicly available information on the Internet in a way that does ***not*** require a person to provide identifying information (such as an email address) as a condition of access and does not involve communication with a human being.
- Approval depends on the activity
  - No specific level of approval
  - AFOSI/CC or delegee
  - AFOSI/CC or single delegee

Procedure 10, UDP

- **Standards for review and approval: approving official must make the following determinations:**
  - **The potential benefits to national security outweigh any adverse impact on civil liberties or privacy of U.S. persons.**
  - **The proposed UDP complies with the limitations on UDP; and**
  - **The proposed UDP is the least intrusive means feasible and conforms to the requirements of Procedure 2.**

Procedure 10, UDP

- UDP requiring no specific level of approval
  - Education or training
  - Cover Activities: Participation in an organization solely for the purpose of obtaining or renewing membership status *in accordance with DoD cover policy*
  - Published or posted information: Participation in an organization whose membership is open to the public solely for the purpose of obtaining information published or posted by the organization or its members and generally available to members; must not involve elicitation.
  - Public forums: Employment affiliation not required and no elicitation of USPI; and
  - Foreign entity

Procedure 10, UDP

- **UDP That May Be Approved by a DIC Head or Delegee**
  - **Non-U.S. persons as potential sources of assistance**
  - **Public forums: employment affiliation required or elicitation of USPI may be authorized**
  - **Cover activities beyond obtaining or renewing membership for the purpose of maintaining or enhancing cover**
  - **U.S. person organizations outside the United States involving participation from or about a non-U.S. person located outside the United States.**

Procedure 10, UDP

- **UDP That May Be Approved by a Defense Intelligence Component Head or a Single Delegee**
  - To conduct authorized CI activities not otherwise addressed in or outside the United States, after required coordination with the FBI or CIA.
  - To collect information inside the United States necessary to identify a U.S. person as a potential source of assistance to foreign intelligence or CI activities.
  - To collect information outside the United States necessary to assess a U.S. person as a potential source of assistance to foreign intelligence or CI activities.

Cyber Authorities

- Data at Rest
  - The Stored Communications Act (SCA)
- Live data
  - Pen Register/Trap & Trace Act
  - The Wiretap Act

Stored Communications Act

- Stored Communications Act (SCA), 18 U.S.C. §§ 2701-2712
  - Provides statutory and procedural protections to customer records and contents of communications when held in electronic storage
  - Electronic storage: "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof"
- Applies to all electronic communications services, e.g., Yahoo, Google, and military networks

Stored Communications Act

- § 2701 prohibits ***unauthorized access*** to stored communications
- Service provider exception
  - Allows person or entity providing a wire or electronic communications service to access stored communications, e.g., sys ads
- Q: Ever wonder how Google knows that you're in the market for . . . a feng shui brass rooster?

Stored Communications Act

- § 2702. Disclosure of Contents
  - Prohibits a person or entity providing an electronic communication service [ECS] ***to the public*** from releasing the contents of a communication while in electronic storage by that service; and
  - Prohibits a person or entity providing remote computing service [RCS] ***to the public*** from releasing the contents of any communication which is carried or maintained on that service

Stored Communicatio!

- Strict requirements apply to public service providers only, per 18 U.S.C. § 2702
- DoD is not a public service provider. See Andersen Consulting LLP v. UOP, 991 F. Supp. 1041 (N.D. IL 1998)
- In theory, no substantial limits for DoD system admins when accessing s communications on our networks

Stored Communications Act

- To gain access to most records of interest, LE needs to either obtain a ***search warrant*** or a § 2703(d) order (used when the records are "relevant and material to an ongoing criminal investigation")
- These must be obtained from a "court of competent jurisdiction"
  - Excludes military courts

SCA, Compelled Disclosure, 18 USC § 2703

Information Sought	Public Provider	Non-Public
Basic subscriber, session, and billing information	Subpoena; 2703(d) order; or search warrant § 2703(c)(2)	Subpoena; 2703(d) order; or search warrant § 2703(c)(2)
Other transactional and account records	2703(d) order or search warrant § 2703(c)(1)	2703(d) order or search warrant § 2703(c)(1)
Retrieved communications and the content of other stored files	Subpoena with notice; 2703(d) order with notice; or search warrant § 2703(b)	Subpoena; SCA does not apply § 2711(2)
Unretrieved communications, including email and voice mail (in electronic storage *more than 180 days*)	Subpoena with notice; 2703(d) order with notice; or search warrant § 2703(a), (b)	Subpoena with notice; 2703(d) order with notice; or search warrant § 2703(a), (b)
Unretrieved communications, including email and voice mail (in electronic storage *180 days or less*)	Search warrant § 2703(a)	Search warrant § 2703(a)

SCA Practice Tips

If an electronic communication may contain evidence relevant to the investigation:

- **Immediately send a preservation request to the provider (renew for 90 days)**
- **Work with local US Attorney's office to obtain a search warrant or court order from a Federal District Court**
- **For subscriber information, i.e., non-content, trial counsel and/or DoD IG subpoena is sufficient**

Real-Time "Live" Data

- Pen Register / Trap & Trace (non-content)
- Wiretap Act (content)

Pen Register / Trap & Trace

- Pen/Trap captures all ***non-content*** information in a communication, i.e., meta data (address on an envelope)
  - Requires a court order, unless an exception met

- Initially applied to telephones only
  - Pen Register: records numbers dialed *from* a particular phone, e.g., 867-5309
  - Trap & Trace: records what numbers dialed *to* a particular phone, i.e., caller ID

- Now includes land lines, cell phones, internet user accounts, email accounts, and IP addresses

Pen Register / Trap & Trace

- Permits providers or wire communication services authority to use pen/trap devices on their own networks without a court order
  - Perform operation, maintenance, and testing
  - Protect provider's property
  - Protect users from abuse / unlawful use of service

- On AFIN, would also apply to "proxy logs" containing records of web page activity

Wiretap Act

The Wiretap Statute

- **Federal Wiretap Statute, 18 U.S.C. § 2510-2520**
  - **BLUF: Wiretapping is illegal, unless an exception applies**
  - **Broadly prohibits eavesdropping everywhere by people in the US (not just the government)**
  - **Wiretap defined: *intercepting communications* using an electronic, mechanical, or other device**
    - **"Communications" means content**
    - **"Intercept" means acquiring contemporaneously with transmission, i.e., "live or real-time" communication**
    - **Applies to Internet communications**
  - **Air Force is a provider of electronic communications services**

Wiretap Statute Exceptions

- Consent, § 2511(2)(c)-(d)
- Accessible to the public, § 2511(2)(g)(i)
- Court order, § 2518
- Service Provider Exception, § 2511(2)(a)(i)
- Computer Trespasser Exception, § 2511(2)(i)
- Extension telephone exception, § 2510(5)(a)
- Inadvertently obtained criminal evidence, § 2511(3)(b)(iv)

Service Provider Exception

- Applies to "provider[s] of electronic communication services"
- System providers are authorized to intercept, disclose, or use network communications to protect rights & property of the provider or to ensure the system continues to provide service
- Allows real-time monitoring w/o a warrant to improve service
  - For example, it is appropriate to scan (intercept) all incoming emails for malicious code, but it is likely not appropriate to scan all emails for certain words.

Computer Trespasser Exception

- This is the primary exception used by LE/CI (AFOSI), 18 USC § 2511
  - Investigators may monitor a computer trespasser if:
    - System owner consents
    - Part of a lawful investigation (AFOSI);
    - *Reasonable grounds* exist to believe the contents of trespasser's communications will be relevant to the investigation; and
    - Interception is limited only to those communications "to and from the trespasser"
  - A trespasser does not include a lawful user of the system who exceeds their authorized access, i.e., "insider threat"
- AFOSI/JA will provide legal advice and staff to AFOSI/CC

Final Thoughts

- **Fourth Amendment violation where GPS was attached to a car without a warrant and Joneses' movements were tracked for 28 days. United States v Jones, 132 S. Ct. 945 (2012)**
  - **"More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." J. Sotomayer, concurring.**

Final Thoughts

- Search of a cell phone incident to arrest requires a warrant. Riley v. California, 134 S. Ct. 2473 (2014).
  - "Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form-unless the phone is." (emphasis in original)

Recap

- What is "cyber law"?
- Reasonable Expectation of Privacy
- Search and Seizure on the AFNET
- Stored Communications Act
- Pen Register / Trap Trace
- Wiretap Act
- Final Thoughts

Stored Communications Act

- **Stored Communications Act (SCA), 18 U.S.C. §§ 2701-2712**
  - **Provides statutory and procedural protections to customer records and contents of communications when held in electronic storage**
  - **Electronic storage: "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof"**
- **Applies to all electronic communications services, e.g., Yahoo, Google, and military networks**

Topics

Status

- February 2016: DoD SIOO sends out 5240.01M for informal coord ✓
- February – March 2016: Working and DoJ adjudicate approximately 170 comments from informal coord ✓
- 7 March 2016: "Clean" 5240.01M sent to WHS for formatting ✓
- 11/14 March 2016: SIOO to send 5240.01M for formal coord ✓
- 1 April 2016: Suspense for formal coord ✓
- 15 April 2016: Complete adjudication of comments (DoD, DoJ) ✓
- April – May 2016: Legal/security/PCLOB reviews ✓
- July 2016: Anticipated signing by AG and SECDEF

Overview

- 5240.01M remains DoD implementing policy for E.O. 12333
- Follows same structure as 5240.1-R
  - Procedure 1 – General Provisions
  - Procedure 2 – Collection
  - Procedure 3 – Retention
  - Procedure 4 – Dissemination
  - Procedure 5 – Electronic Surveillance
  - Procedure 6 – Concealed Monitoring
  - Procedure 7 – Physical Search
  - Procedure 8 – Mail Searches and Cover
  - Procedure 9 – Physical Surveillance
  - Procedure 10 – Undisclosed Participation
- Procedures 11 – 15 removed from 5240.01M; AG approval not needed
  - To be published in other DoD issuance

Key Changes

- **New definition of collection**
  - Information is collected when it is received
  - Exception is when information not intelligible (e.g. encrypted)
  - Dissemination received from another agency is NOT collection
- **Concepts of shared repository and special collection added**
- **Counterintelligence exception expanded to account for HVE**
- **New retention timeframes for incidental collection**
  - Domestic incidental collection may be retained up to five years
  - Overseas incidental collection may be retained up to 25 years
  - DIC Heads and single delegee may approve extensions

Key Changes

- **Military magistrates may no longer authorize Procedure 7**
  - Only MCIOs may conduct searches against AD personnel
  - Must obtain FISA
- **Three approval levels for UDP**
  - No specific approval
  - DIC Head or delegee(s)
  - DIC Head or single delegee
- **Definitions of organization in US and outside US expanded to account for internet activity**
- **List of Defense Intelligence Components and their heads updated**

MAJOR CHANGES BY PROCEDURE

Procedure 1

General Provisions

Procedure 1 – General Provisions

- Para 3.1.b. – Adds concept of shared repositories
  - Para 3.1.b.2. – Procedures for components hosting shared repositories
  - Para 3.1.b.3. – Procedures for components acting as participants in shared repositories
- Paras 3.1.c. – 3.1.e. – DoD Senior Intelligence Oversight Official (SIOO) added as cognizant entity for interpretation, exceptions, amendments to 5240.01M

Procedure 2

Collection of US Person Information

Procedure 2 – Collections

- Para 3.2.c.4.c. – Counterintelligence: exception expands foreign terrorist connection to include individuals "*reasonably believed to be acting for or in furtherance of, the goals or objectives of an international terrorist or international terrorist organization, for purposes harmful to the national security of the United States.*"
    - Permits collection when no specific connection to foreign terrorist(s) has been established – HVE (e.g. San Bernardino, Orlando)

- Para 3.2.c.5.b. – Threats to Safety: Allows DIC heads or delegee to authorize collection when they have determined a "*persons' life or physical safety is reasonably believed to be in imminent danger;*"

Procedure 2 – Collections

- Para 3.2.c.8. – Persons in Contact With Sources or Potential Sources: New exemption category added.

- Para 3.2.c.10. – Physical Security: This exemption now includes a requirement that there exist a "*reasonable belief in…the foreign connection of the U.S. persons…and the physical security threat they pose.*"

- Para 3.2.c.12. – Overhead and Airborne Reconnaissance: This exemption now includes requirements to comply with DoD or NGA policies and procedures

- Former exemption for Narcotics has been removed (replaced by 3.2.c.8.)

Procedure 2 – Collections

- Para 3.2.e. – Adds notion of Special Circumstances Collection
  - "(C)*ollection opportunities raise special circumstances based on the volume, proportion, and sensitivity of the USPI likely to be acquired, and the intrusiveness of the methods used to collect the information.*"
  - DIC head or delegee must approve such collection and report approval to DoD SIOO
- Para 3.2.f.3. – Requires that in any collection of non-publicly available information the DICs must "*to the extent practicable, take steps to collect no more information that is reasonably necessary.*"

Procedure 3

Retention of US Person Information

Procedure 3 – Retention

- Para 3.3.c.1. – Intentional Collection of USPI: DIC must evaluate information promptly, but may retain for up to five years for evaluation
    - DIC Head or single delegee may approve an extended period
- Para 3.3.c.2.a. – Information collected incidentally in the US, or about a place in the US, may be retained for five years for evaluation
    - DIC Head or single delegee may approve an extended period
- Para 3.3.c.2.b. - Information collected incidentally outside the US, or about a place outside the US, may be retained for 25 years for evaluation
    - DIC Head or single delegee may approve an extended period

Procedure 3 – Retention

- Para 3.3.c.3. – Voluntarily Provided USPI: DIC may retain such information for up to five years for evaluation
    - DIC Head or single delegee may approve an extended period
    - If DIC receives voluntarily provided information about individual believed to be a non-US Person, but info may contain USPI, retention period is 25 years
- Para 3.3.c.4. – Special Circumstances: Such information may be retained for up to five years
    - USD(I) may approve an extended period
- Para 3.3.c.5. – Extended Retention

Procedure 3 – Retention

- Para 3.3.c.6. – Retention time frames do not begin until information has been processed into intelligible form (e.g. decryption)

- Para 3.3.d. – Information received from another component or IC element will be subject to the same, concurrent retention time limits as originating agency (i.e. clock does not restart for receiving entity)

- Para 3.3.e. – Addresses criteria for permanent retention

- Para 3.3.f.1.b. – Requires that "*when retrieving information electronically, tailor queries…to the greatest extent practicable to minimize the amount of USPI returned that is not pertinent…*"

- Para 3.3.f.1.c. – DICs must "*take reasonable steps to audit access to information systems containing USPI and to audit queries…to assess compliance with this issuance.*"

Procedure 3 – Retention

- Para 3.3.f.1.d. – When developing and implementing information systems for use with USPI, DICs must "*take reasonable steps to ensure effective auditing and reporting…*"
- Para 3.3.f.1.e. – When retaining information DICs are required to "*(e)stablish documented procedures for retaining data containing USPI and recording the reason…and the authority approving the retention.*"
- Para 3.3.f.1.f. – Requires annual training for employees accessing or using USPI
- Para 3.3.f.2. – DICs must employ reasonable measures to identify and mark files containing USPI
- Para 3.3.f.3. – DoD SIOO will periodically review DIC practices

Procedure 3 – Retention

- Para 3.3.g. – Enhanced Safeguards: DIC Head or delegee must assess need for enhanced safeguards when there is special circumstances collection
    - Factors to consider include
        - Intrusiveness of collection method(s)
        - Volume or sensitivity of USPI
        - Potential for harm, embarrassment, inconvenience, unfairness
        - Uses of USPI being retained
        - Length of retention
    - Para 3.3.g.2. – Details potential enhanced safeguard measures

Procedure 4

Dissemination of US Person Information

Procedure 4 – Dissemination

- Para 3.4.c. – Criteria for Dissemination: Several new categories added
    - Para 3.4.c.1. – Any Person or Entity: Dissemination to any person or entity permitted if information is publicly available or collected via consent
    - Para 3.4.c.8. – Protective Purposes: Dissemination permitted if necessary to protect safety/security of persons or property, or to protect against crime or threat to national security
- Para 3.4.d. – DICs may disseminate large amounts of unevaluated USPI (defined in Para 3.4.c.3.) with approval of DIC Head or single delegee, after notification to DoD SIOO

Procedure 4 – Dissemination

- Para 3.4.e. – DICs should not include USPI in dissemination "*if pertinent information can be conveyed in an understandable way without including the identifying information.*"
    - If dissemination includes USPI the receiving entity must be so notified
- Para 3.4.g. – Special considerations/controls on dissemination of information to the White House
- Para 3.4.h. – DICs must have procedures in place to address improper dissemination of USPI

Procedure 5

Electronic Surveillance

Procedure 5 – Electronic Surveillance

- Para 3.5.c.2. – Adds Attorney General (AG) to Foreign Intelligence Surveillance Court (FISC) as authorizing entities for electronic surveillance in the US
    - Paras 3.5.c.2.a. and 3.5.c.2.b. add criteria which DICs must meet in order to conduct such surveillance
- Para 3.5.c.3. – Add USD(I) as DoD entity authorized to request electronic surveillance of US Person in US
- Para 3.5.d.3. – Add USD(I) as DoD entity authorized to request electronic surveillance of US Person outside US
- Para 3.5.e. – Does NOT apply to MCIO CI activities against non-US Persons outside of the US

Procedure 5 – Electronic Surveillance

- Para 3.5.g. – In emergency situations, DICs may obtain approval from AG
    - Request for AG approval must be made by
        - SECDEF/DEPSECDEF
        - USD(I)
        - SECAF/USECAF (SECNAV/USECNAV, SECAR/USECAR)
        - DIRNSA
- Para 3.5.h. – In exigent circumstances, DICs may target US Persons outside of the US when AG approval is not practical if:
    - Person's life or physical safety in danger; or
    - Physical security of USG property in danger from foreign power; or
    - Time required for AG approval would result in harm to national security

Procedure 5 – Electronic Surveillance

- Para 3.5.h.2. – Approval of exigent circumstance electronic surveillance limited to :
  - SECDEF/DEPSECDEF
  - USD(I)
  - SECAF/USECAF (SECNAV/USECNAV, SECAR/USECAR)
  - DIRNSA/Deputy DIRNSA
  - NSA SIGINT Director
  - DIRNSA Senior Representative
  - Any flag/general office at overseas location in question w/responsibility for subject or endangered resources
- Para 3.5.i.2.b.1. – Adds allowance for collection of incidental information during TSCM when it is not reasonable to obtain consent of persons subject to incidental collection

Procedure 5 – Electronic Surveillance

- Para 3.5.i.2.c. – Adds criteria for retention and dissemination of information obtained during TSCM

- Para 3.5.i.3.c. – Adds several permissible targets of electronic surveillance for training purposes (sub-paras 3, 4, 5 and 6)

- Para 3.5.i.3.d. – Lists five conditions which must be met to train against targets other than those listed in 3.5.i.3.c.

    - Surveillance not targeted at particular person without consent
    - Not reasonable to obtain consent of persons incidentally subjected to surveillance
    - Not reasonable to train without engaging in such surveillance
    - Surveillance limited in extent and duration to that necessary
    - Minimal acquisition of information permitted for calibration

Procedure 6

Concealed Monitoring

Procedure 6 – Concealed Monitoring

- Para 3.6.a.2. – Procedure does not apply to concealed monitoring for testing or training when subjects consent; otherwise subject to Procedure 6

- Para 3.6.c.1. – DICs may conduct concealed monitoring outside DoD facilities in the US after coordination with FBI and in accordance with all DoJ/FBI agreements

- Para 3.6.c.3. – Concealed monitoring may be approved by DIC Head or a delegee

Procedure 7

Physical Searches

Procedure 7 – Physical Searches

- **NOTE: Searches based upon military magistrate authorization pursuant to Military Rules of Evidence are no longer permitted under Procedure 7**
  - Search authorizations may be used to pursue potential UCMJ violations under Military Rules of Evidence
- Para 3.7.c. – Searches Against Active Duty Military Personnel: only MCIOs may be authorized to conduct
  - Must be conducted under FISA with AG or FISC approval
  - SECDEF/DEPSECDEF, USD(I), SECAF/USECAF may seek approval
  - In emergency situations MCIO Head or delegee may make request to DoD GC to seek AG authorization

Procedure 7 – Physical Searches

- Para 3.7.d. – Searches Against Other Persons in the US: DICs may not conduct, but may request FBI to conduct if two conditions met

  1. Search must be for authorized FI or CI purpose

  2. Search must meet definition of physical search under FISA

  - SECDEF/DEPSECDEF, USD(I), SECAF/USECAF, DIRNSA, Director DIA, Director NGA, Director NRO may seek approval

  - In emergency situations MCIO Head may make request to DoD GC ask FBI to conduct search

Procedure 7 – Physical Searches

- Para 3.7.e. – Searches of Other US Persons or Their Property Outside the US: DICs may conduct such searches if three conditions met

  1. Search is for authorized FI or CI purpose; and

  2. Search is appropriately coordinated with CIA; and

  3. FISC or AG has approved search

  - SECDEF/DEPSECDEF, USD(I), SECAF/USECAF, DIRNSA, Director DIA, Director NGA, Director NRO may seek approval

  - In emergency situations MCIO Head may make request to DoD GC to seek AG authorization

Procedure 8

Searches of Mail and Mail Covers

Procedure 8 – Searches of Mail and Mail Covers

- Para 3.8.a. – Clarifies that this Procedure does not apply to items transported by a commercial carrier (e.g. Federal Express, UPS, etc.)

- Para 3.8.c.1. – Searches of Mail: subject to Procedure 7 limitations and approvals

- Para 3.8.d. – Mail covers: DICs may request USPS conduct mail cover for items in USPS channels

    - For mail in foreign channels DICs may request mail cover for items to/from US Person in accordance with local law and SOFA

    - No specific DIC official(s) identified as required to make request

Procedure 9

Physical Surveillance

Procedure 9 – Physical Surveillance

- Para 3.9.c.1.a. – DICs may conduct surveillance of US Persons in US if they fall into the existing 5240.1-R categories
- Para 3.9.c.1.b. – DICs may conduct surveillance of non-US Persons in US for authorized FI or CI purpose
- Para 3.9.c.1.c. – DIC Head or delegee must approve authorized physical surveillance
  - Physical surveillance in the US must be coordinated with FBI per existing agreements with DoJ/FBI
  - DICs can participate in physical surveillance of other US Persons in US when detailed to, or operating under the authorities of, the FBI

Procedure 9 – Physical Surveillance

- Para 3.9.c.1.d. – DIC Head or delegee may approve DIC participation in authorized FBI physical surveillance in US when FBI requests and authorizes DIC participation in writing

- Para 3.9.c.2.c. – DIC Head or a delegee may approve physical surveillance of any US person outside of the US

  - Physical surveillance outside the US conducted off of a military installation must be coordinated with the CIA

  - Approving official must consider host nation laws and SOFA

Procedure 10

Undisclosed Participation

Procedure 10 – Undisclosed Participation

- Para 3.10.a. – Clarifies that Procedure 10 applies to sources
- Para 3.10.b. – Identified three categories of excluded activities
  - Personal participation (i.e. undertaken for personal reasons and at personal expense)
  - Voluntarily provided information from existing members without request from DIC
  - Publicly available information on the internet collected in such a way that provision of personal identifying information is not required, and no communication with human being occurs

Procedure 10 – Undisclosed Participation

- Para 3.10.e. – Limitations on Undisclosed Participation: adds two additional limitations not found in 5240.1-R
    - UDP may not be authorized to collect on domestic activities of US persons
    - All UDP must be coordinated with FBI, CIA or other agency in accordance with EO 12333 and other policies/agreements
- Para 3.10.e.6.b. – DICs wishing to engage in UDP to influence activities of an organization per Para 3.10.e.6.a. must make request to USD(I) through DoD/GC
- Para 3.10.e.6.c. – Prohibition on influencing organizations does not apply to non-US Persons located outside the US

Procedure 10 – Undisclosed Participation

- Para 3.10.f. – Required Approvals: Approvals now authorized at three levels

    1. No Specific Approval Required: Recognizes activity as UDP but no specific approval required

        - Education or training
        - Participation to maintain cover; no further activity in organization
        - Information published or posted by an organization open to the public when information is available to all members and no elicitation occurs (e.g. Subscription to Washington Post)
        - Public forums, to include social media, when employment affiliation is not required and no elicitation occurs (e.g. Facebook public profiles)
        - Foreign entities

Procedure 10 – Undisclosed Participation

2. UDP that may be approved by DIC Head or delegee

   - Information collected to identify and assess non-US Person as potential source of assistance

   - Public forums, to include social media, when employment affiliation is required and/or elicitation occurs (e.g. Facebook non-public profiles)

   - Cover activities beyond obtaining or renewing membership

   - Information collected outside the US from or about a non-US Person located outside the US

Procedure 10 – Undisclosed Participation

3. UDP that may be approved by DIC Head or ***single*** delegee

   - Collection of FI outside of US from or about a specific US Person, or from or about a non-US Person in the US
   - To conduct CI activities not addressed previously, in or outside the US
   - Collection of information inside the US needed to identify a US Person as potential source
   - Collection of information outside the US needed to assess a US Person as potential source

- Para 3.10.f.4. – UDP not addressed elsewhere in Procedure may be authorized by USD(I) or DIC Head with notice to DoD SIOO

Procedure 10 – Undisclosed Participation

- Para 3.10.f.5. – Approving official must make following determinations
  - "*Potential benefits to national security outweigh any adverse impact on civil liberties or privacy of US Persons.*"
  - UDP complies with requirements of Para 3.10.e.
  - UDP is least intrusive means feasible to obtain information and conforms to Procedure 2
- Para 3.10.g. – Disclosure requirement: Disclosure of DIC affiliation must be sufficient to apprise appropriate official(s) of the affiliation
  - If official to whom disclosure would be made acting on behalf of DIC, his/her knowledge not sufficient unless senior official of organization
  - DIC will maintain written record of disclosures, including to whom made

Definitions

Definitions

THE FOLLOWING DEFINITION HAVE BEEN ADDED OR NOTABLY CHANGED FROM 5240.1-R
(Definitions below are summarized)

- Agent of a Foreign Power – any person, including a US Person, acting for or on behalf of a foreign power
- Collection – information is collected ***when it is received by a DIC***
- Defense Intelligence Components – now defined as:
  - NSA/CSS
  - DIA
  - NRO
  - NGA
  - FI and CI elements of the Military Departments
  - Senior Intelligence Officials of the COCOMs

Definitions

- Defense Intelligence Component Head – now includes:
  - Director NSA
  - Director DIA
  - Director NRO
  - Director NGA
  - Deputy Chief of Staff, G2, Department of the Army
    - Commander, Army INSCOM
  - Director of Naval Intelligence
    - Director of Naval Intelligence Activity
    - Commander, ONI
  - Commander, US Fleet Cyber Command
  - Director, NCIS
  - Director of Intelligence, USMC
  - Commander, Marine Corps Intelligence Activity
  - Deputy Chief of Staff, ISR, Department of the Air Force
    - Commander, 25th Air Force
  - Commander, AFOSI

Definitions

- Detail – an employee of one agency operating under the authorities of another agency
- Dissemination – transmission of information outside of a DIC
- DoD Facility – Installations/facilities owned, leased or occupied by accommodation by DoD
- Foreign Connection – US Person in contact with a foreign person for purposes harmful to US national security
- Host of a Shared Repository – entity maintaining a shared repository
- Imagery – likeness of any feature and positional data thereof
- Incidental Collection of USPI – USPI collection not deliberately sought by a DIC but which is nonetheless collected
- Intelligence – includes FI and CI

Definitions

- Intentional Collection of USPI – USPI collection deliberately sought by a DIC
- Organization – expanded to include entities which meet and communicate principally through the use of technology
- Organization in the US – expanded to include organizations primarily meeting via the internet substantially composed of persons located in the US
- Organization Outside the US Constituting a US Person - organization physically located outside the US but substantially composed of US Persons or organization primarily meeting via the internet substantially composed of US Persons located outside the US
- Overhead Reconnaissance – activities of space-based capabilities conducting imagery collection

Definitions

- Physical Search – expanded to include electronic data
- Shared Repository– database or other repository maintained for the use of more than one agency
- Transmission Media Vulnerability Survey– acquisition of transmissions to determine vulnerability to interception
- Undisclosed Participation – participation in an organization without disclosure of DIC affiliation
- USPI – information reasonably likely to identify a specific US Person

Definitions

THE FOLLOWING DEFINITION HAVE BEEN REMOVED FROM 5240.01M

- Counterintelligence Investigation
- Lawful Investigation
- Physical Security
- Physical Security Investigation
- Signals Intelligence

QUESTIONS?

Air Force Office of Special Investigations

Eyes of the Eagle

DoDM 5240.01 Legal Primer

29 Sept 2016

U.S. AIR FORCE

Topics

- DoDM 5240.01 Overview
- DoDM 5240.01 Procedures
  - Proc 2, Collection
  - Proc 3, Retention
  - Proc 4, Dissemination
  - Proc 5, Electronic Surveillance
  - Proc 6, Concealed Monitor
  - Proc 7, Physical Search
  - Proc 8, Mail Search/Cover
  - Proc 9, Physical Surveillance
  - Proc 10, Undisclosed Participation
- JA Checklist

DoDM 5240.01, Overview

DoD MANUAL 5240.01

PROCEDURES GOVERNING THE CONDUCT OF DoD INTELLIGENCE ACTIVITIES

Originating Component:	Office of the Deputy Chief Management Officer of the Department of Defense
Effective:	Month Day, Year
Releasability:	Cleared for public release. Available on the DoD Issuances Website at http://www.dtic.mil/whs/directives
Incorporates and Cancels:	Directive-type Memorandum 08-052, "Intelligence Oversight Policy Guidance," March 26, 2008 Procedures 1-10 of DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 7, 1982
Approved by:	Loretta E. Lynch, Attorney General of the United States Ashton B. Carter, Secretary of Defense

Purpose: In accordance with the authority in DoD Directive 5240.01 and Executive Order (E.O.) 12333, this issuance:

- Establishes procedures to enable DoD to conduct authorized intelligence activities in a manner that protects the constitutional and legal rights and the privacy and civil liberties of U.S. persons. DoD authorized intelligence activities are foreign intelligence and counterintelligence (CI) activities unless otherwise specified in this issuance.
- Authorizes the Defense Intelligence Components to collect, retain, and disseminate information concerning U.S. persons in compliance with applicable laws, Executive orders, policies, and regulations.

DoDM 5240.01, Overview

- Effective 8 Aug 2016; signed by SecDef and AG
- Changes are substantial, but not significant
- Replaces Procedures 1-10 of DoD 5240.1-R (Dec 1982)
- DoD 5240.01-R, Procedures 11-15, remain in effect
- No changes to Executive Order 12333

DoDM 5240.01, Overview

- CI Defined: Information gathered and activities conducted to *identify, deceive, exploit, disrupt,* or *protect* against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

Procedure 2, Collection—Introduction

- **Intentional Collection of USPI: We may *intentionally* collect USPI *only* if:**
  - the information sought is ***reasonably believed;***
  - to be *necessary* for the performance of an authorized CI mission; and
  - the USPI falls within one of the following 13 categories below.
    - CI2MS *requires* that you indicate a Proc 2 collection category

- **U.S. Person Information (USPI) defined: Information that is reasonably likely to identify one or more specific U.S. persons.**

- **Collection takes place upon receipt**
  - Regardless of when you use it
  - Computers can collect
  - Intel is collected only once
  - May be disseminated multiple times
  - Encrypted data is considered collected upon receipt

Procedure 2, Collection—Reasonable Belief

- **Defined: When the facts and circumstances are such that a reasonable person would hold the belief.**
  - **Must rest on facts and circumstances that can be articulated;**
  - **Hunches or intuitions are not sufficient; and**
  - **Can be based on experience, training, and knowledge of CI activities as applied to particular facts and circumstances.**

Procedure 2, Collection—Categories

1. Publicly Available
2. Consent
3. Foreign Intelligence (FI)
4. Counterintelligence (CI)
5. Threats to Safety
6. Protection of Sources/Methods
7. Current, Former, or Potential Sources
8. Persons in Contact With Sources or Potential Sources
9. Personnel Security
10. Physical Security
11. Communications Security
12. Overhead and Airborne Reconnaissance
13. Administrative Purposes

Procedure 2, Collection Categories

1. **Publicly Available Information**

2. **Consent**
   - **The legal advisor must determine whether a notice or policy is adequate and lawful, before the Component takes or refrains from taking action on the basis of implied consent (DoDM 5240.01, G.2.)**

3. **Foreign Intelligence**
   - **AFOSI does not have a foreign intelligence mission**

Procedure 2, Collection—Categories

4. Counterintelligence: The information is reasonably believed to constitute CI and the U.S. person is one of the following:

(a) An individual, organization, or group reasonably believed to be engaged in or preparing to engage in espionage, other intelligence activities, sabotage, or assassination on behalf of a *foreign* power, organization, or person, or on behalf of an agent of a *foreign* power, organization, or person;

(b) An individual, organization, or group reasonably believed to be engaged in or preparing to engage in international terrorist activities;

(c) An individual, organization, or group reasonably believed to be acting for, or in furtherance of, the goals or objectives of an international terrorist or international terrorist organization, for purposes harmful to the national security of the United States; or

(d) An individual, organization, or group *in contact with a person described above* for the purpose of identifying such individual, organization, or group and assessing any relationship with the person described therein.

Procedure 2, Collection—Categories

5. Threats to safety: information needed to protect the safety of any person or organization, including those who are targets, victims, or hostages of international terrorist organizations, if:

- **The threat has a foreign connection;**
- **AFOSI/CC or delegee has determined that a person's life or physical safety is reasonably believed to be in imminent danger; *or***
- **The information is needed to maintain maritime or aeronautical safety of navigation.**

Procedure 2, Collection—Categories

6. **Protection of Intelligence Sources, Methods, and Activities**
   - The information is about U.S. persons who have access to, had access to, will have access to, or are otherwise in possession of information that reveals foreign intelligence or CI sources, methods, or activities, when collection is **reasonably believed** necessary to protect against the unauthorized disclosure of such information.

7. **Current, Former, or Potential Sources of Assistance**
   - The information is about those who are or have been sources of information or assistance, or are **reasonably believed** to be potential sources of information or assistance, to intelligence activities for the purpose of assessing their suitability or credibility.

8. **Persons in Contact With Sources or Potential Sources**
   - The information is about persons in contact with sources or potential sources, for the purpose of assessing the suitability or credibility of such sources or potential sources.

9. **Personnel Security**
   - The information is arising from a lawful personnel security investigation.

Procedure 2, Collection—Categories

10. Physical Security

- The information is about U.S. persons **reasonably believed** to have a *foreign* connection and who pose a threat to the physical security of DoD personnel, installations, operations, or visitors.
- Must have or be supporting an authorized physical security mission and must be able to articulate a **reasonable belief** in both the foreign connection of the U.S. persons who are collection targets and the physical security threat they pose.

11. Communications Security Investigation

- The information is arising from a lawful communications security investigation.

Procedure 2, Collection—Categories

12. Overhead and Airborne Reconnaissance

- May intentionally collect imagery that contains USPI provided that the collection is ***not*** directed at a specific U.S. person or, if the collection is directed at a specific U.S. person, the collection falls in one of the other 12 categories
- Includes information obtained from unmanned aircraft systems
- See SecDef Memo Feb 2016

13. Administrative Purposes

Procedure 2, Collection—Other Considerations

- **Least Intrusive Means**
  - Use the least intrusive collection techniques feasible within the United States *or* directed against a U.S. person abroad.
    1. Publicly available sources or with consent
    2. Cooperating sources
    3. Techniques that do *not* require a judicial warrant or AG approval
    4. Techniques that do require a judicial warrant or AG approval
- **Amount of Information Collected**
  - In collecting non-publicly available USPI, to the extent practicable, collect no more information than is reasonably necessary.
- **Special Circumstances Collection [BIG data]**
  - Components will consider whether collection opportunities raise special circumstances based on the *volume*, *proportion*, and *sensitivity* of the USPI likely to be acquired, and the intrusiveness of the methods used to collect the information.

Procedure 3, Retention

- **Permanent Retention standard**
  - **Retention is reasonably believed to be necessary for the performance of an authorized intelligence mission; *and***
  - **The information was lawfully collected or disseminated to the Component:**
    - **Meets one of the 13 Proc 2 collection categories; or**
    - **Is necessary to understand or assess CI, e.g., information about a U.S. person that provides important background or context for CI.**

Procedure 3, Retention

- Three primary evaluation periods to determine permanent retention of USPI
  - Promptly
  - Five (5) years
  - Twenty-five (25) years

- Intentional Collection of USPI
  - Must be evaluated promptly; and
  - If *necessary*, may retain the information for evaluation for up to 5 years, subject to extension

Procedure 3, Retention

- **Incidental Collection of USPI**
  - Defined: collection of USPI that is not deliberately sought, but is nonetheless collected
  - *In the United States,* may retain all of the incidentally collected information for evaluation for up to 5 years, unless extended
  - *Outside the United States, may* retain all of the incidentally collected information for evaluation for up to 25 years

- **Voluntarily Provided USPI**
  - About a U.S. person, evaluate the information promptly, up to 5 years, unless extended
  - About a non-U.S. person, evaluation for up to 25 years

Procedure 3, Retention

- **Unintelligible information**
  - Includes information that a Component cannot decrypt or understand in the original format
  - The time periods begin when the information is processed into intelligible form
  - To the extent practicable, unintelligible information will be processed into an intelligible form
  - A foreign language is considered intelligible

- **Deletion of Information**
  - Unless the standards for permanent retention are met, must delete all USPI from the Component's automated systems of records

Procedure 4, Dissemination

- We may disseminate USPI based upon the following criteria:
  - Any person or entity: Information is publicly available or U.S. person has consented to the dissemination
  - Other intelligence community elements
  - Other DoD elements; federal government entities; state, local, tribal, or territorial governments: recipient is **reasonably believed** to have a need to receive such information for the performance of its lawful missions or functions.
  - Foreign governments or international organizations
    - Recipient is **reasonably believed** to have a need to receive such information for its lawful missions or functions; and
    - Disclosure is consistent with applicable international agreements and foreign disclosure policy
  - Protective Purposes
    - Necessary to protect the safety or security of persons or property, or to protect against or prevent a crime or threat to the national security

Procedure 5, Electronic Surveillance

- Implements FISA and E.O. 12333
- Defined for U.S. collection
  - The installation or use of any monitoring device in the United States where a person has a reasonable expectation of privacy, as determined by JA, and
  - A warrant would be required for law enforcement purposes
- Fourth Amendment
  - All electronic surveillance must comply with the Fourth Amendment
  - JA must assess the reasonableness of collection, retention, and dissemination (DoDM 5240.01, para. 3.5.b.)

Procedure 5, Electronic Surveillance

- **In the United States**
  - **Attorney General or the Foreign Intelligence Surveillance Court (FISC) must authorize, except in emergency situations.**
  - **May only conduct such surveillance if both:**
    - **A *significant purpose* of the electronic surveillance is to obtain foreign intelligence information; and**
    - **There is probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power.**

Procedure 5, Electronic Surveillance

- Outside the United States
  - U.S. person
    - Governed by FISA and E.O. 12333; or
    - Approval under exigent circumstances exception
  - Non-U.S. person: governed by Title I or Section 702
- Emergency situations: Attorney General approval
- Technical Surveillance Countermeasures (TSCM)
  - Applies to the use of electronic equipment and specialized techniques to determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance.

Procedure 6, Concealed Monitoring

- **Defined as the following:**
  - Hidden electronic, optical, or mechanical devices,
  - to monitor a particular person or a group of persons,
  - without *consent*,
  - in a surreptitious manner,
  - over a period of time, and
  - no *reasonable expectation of privacy*
- **Examples**
  - Video monitoring or sound recording of a subject in a place where he or she has no reasonable expectation of privacy if conducted over a period of time
  - Taking one photograph of a subject would *not* qualify

Procedure 6, Concealed Monitoring

- Scope
  - *Any* person inside the United States, or
  - Any U.S. person outside the United States

- Procedures
  - In the United States
    - On DoD facilities
    - Outside DoD facilities, after coordination with the FBI
  - Outside the United States
    - On DoD facilities
    - Outside DoD facilities must be coordinated with the CIA, and appropriate host country officials in accordance with any applicable SOFA or other international agreement.

Procedure 6, Concealed Monitoring

- Approval: AFOSI/CC or delegee (*new*)

- The following criteria must be met:
  - There is no reasonable expectation of privacy;
  - Such monitoring is necessary to conduct an assigned CI function;
  - A trespass will not be necessary to effect the monitoring; and
  - The monitoring is not subject to Procedure 5 (DoDM 5240.01, 3.6.c.(3))

Procedure 7, Physical Searches

- Scope: Applies to *nonconsensual* physical searches in the United States ***and*** of U.S. persons/property outside the United States.
- Defined: Any intrusion on a person or property that would require a *warrant* for law enforcement purposes.
- Does ***not*** include examinations of
  - Areas that are in plain view;
  - Publicly available information;
  - Abandoned property in a public place;
  - Items where we have consent; and
  - Government property pursuant to Military Rule of Evidence 314(d)

Procedure 7, Physical Searches

- **Active duty**
  - Approval: Attorney General (AG) or FISC (*new*)
- **Other persons inside the United States**
  - We may ***NOT*** conduct searches of other persons
  - We may request the FBI to conduct such a search
- **Other U.S. persons outside the United States**
  - The search is for an authorized foreign intelligence or CI purpose;
  - The search is appropriately coordinated with the CIA; and
  - The FISC or the AG has authorized the search
  - Who can request
    - SecDef, DSD, USD(I); SecAF; USecAF; DIRNSA/CHCSS; Director, DIA; Director, NGA; or Director, NRO

Procedure 8, Mail Searches and Cover

- Mail searches
  - See Procedure 7

- Mail cover
  - In U.S. postal service channels, request the USPS IAW 39 CFR 233.3(e)(2)
  - In foreign postal channels, may request a mail cover for mail that is to or from a U.S. person consistent foreign law and any applicable SOFA

Procedure 9, Physical Surveillance

- **Who can we surveil *in* the United States:**
  - Military service members;
  - Present or former military or civilian employees of a DIC;
  - Present or former contractors of a DIC;
  - Present or former employees of such a contractor;
  - Applicants for such employment or contracting;
  - Non-U.S. persons (*new*); and
  - Other persons
    - "when **detailed** to the FBI, or
    - when operating **under FBI authorities**."
- ***Outside*** **of the United States**
  - "Any U.S. person . . . for an authorized foreign intelligence or CI purpose" (DoDM 5240.01, para. 3.9.c.(2)(a))

Procedure 9, Physical Surveillance

- **Scope**
  - Any person inside the United States or any U.S. person outside the United States.
  - Also applies to any devices used to observe the subject of the surveillance (not Procedure 6).

- **Defined**
  - Deliberate and continuous observation of a person, and
  - Where the person has no reasonable expectation of privacy
  - Does ***not*** apply to surveillance detection or counter surveillance used to detect and elude foreign physical surveillance

Procedure 9, Physical Surveillance

- **Approval and coordination**
  - **Approval: AFOSI/CC or delegee**
  - **Coordination**
    - **In the United States**
      - No coordination req'd for surveillance of active duty, on-base
      - FBI coord for off-base surveillance
      - FBI coord for surveillance on-base, non-active duty
    - **Outside the United States**
      - CIA coord for off-base surveillance
      - Consider with SOFA and foreign law/policy

Procedure 10, Undisclosed Participation (UDP)

- Scope: Governs the ***participation*** by an defense IC and anyone acting on behalf of an IC, e.g., sources, in any ***organization*** in the United States or any organization outside the United States that constitutes a U.S. person.
- Organization defined
  - An association of two or more individuals formed for any *lawful* purpose whose existence is formalized in some manner
  - Includes those that meet and communicate through the use of technologies
- Participation defined
  - When a person is tasked or asked to participate in an organization for the benefit of the DIC
  - Actions undertaken "for the benefit of" a DIC may include collecting information, identifying potential sources or contacts, or establishing or maintaining cover.

Procedure 10, Undisclosed Participation (UDP)

- **Exclusions**
  - Personal participation
  - Voluntarily provided information
  - Publicly available information on the Internet
    - Collection of publicly available information on the Internet in a way that does *not* require a person to provide identifying information (such as an email address) as a condition of access and does not involve communication with a human being
- **Approval level depends on the activity**
  - No specific level of approval
  - AFOSI/CC or delegee
  - AFOSI/CC or single delegee

Procedure 10, Undisclosed Participation (UDP)

- Standards for review and approval:
  - The potential benefits to national security outweigh any adverse impact on civil liberties or privacy of U.S. persons;
  - The proposed UDP complies with the limitations on UDP; and
  - The proposed UDP is the least intrusive means feasible and conforms to the requirements of Procedure 2.

Procedure 10, Undisclosed Participation (UDP)

- UDP requiring no specific level of approval
  - Education or training
  - Cover Activities: Participation in an organization solely for the purpose of obtaining or renewing membership status *in accordance with DoD cover policy*
  - Published or posted information: Participation in an organization whose membership is open to the public solely for the purpose of obtaining information published or posted by the organization or its members and generally available to members; must not involve elicitation.
  - Public forums: Employment affiliation not required and no elicitation of USPI; and
  - Foreign entity

Procedure 10, Undisclosed Participation (UDP)

- **UDP That May Be Approved by a Component Head or Delegee**
  - Non-U.S. persons as potential sources of assistance
  - Public forums: employment affiliation required or elicitation of USPI may be authorized
  - Cover activities beyond obtaining or renewing membership for the purpose of maintaining or enhancing cover
  - U.S. person organizations outside the United States involving participation from or about a non-U.S. person located outside the United States.

Procedure 10, Undisclosed Participation (UDP)

- **UDP That May Be Approved by a Component Head or a *Single* Delegee**
  - To conduct authorized CI activities not otherwise addressed in or outside the United States, after required coordination with the FBI or CIA.
  - To collect information inside the United States necessary to identify a U.S. person as a potential source of assistance to foreign intelligence or CI activities.
  - To collect information outside the United States necessary to assess a U.S. person as a potential source of assistance to foreign intelligence or CI activities.

THE AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS
FREEDOM OF INFORMATION ACT/PRIVACY ACT DELETED PAGE INFORMATION SHEET

5 pages withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Title 5, United States Code (U.S.C.), Section 552 (FOIA)				Title 5, U.S.C. Section 552a (PA)	
☐	(b)(1)	☐	(b)(7)(D)	☐	(d)(5)
☐	(b)(2)	☐	(b)(7)(E)	☐	(j)(2)
☐	(b)(3)	☐	(b)(7)(F)	☐	(k)(1)
☐	(b)(4)	☐	(b)(8)	☐	(k)(2)
☒	(b)(5)	☐	(b)(9)	☐	(k)(3)
☐	(b)(6)	☐		☐	(k)(4)
☐	(b)(7)(A)	☐		☐	(k)(5)
☐	(b)(7)(B)	☐		☐	(k)(6)
☐	(b)(7)(C)	☐		☐	(k)(7)

☐ Documents originated with (an)other Government agency(ies). These documents were referred to that agency for review and direct response to you.

____ pages contain information furnished by (an)other Government agency(ies). You will be advised by AFOSI as to the releasability of this information following our consultation with the other agency(ies).

____ pages have not been provided to you at this time because a final release determination has not been made. You will be advised as to the disposition at a later date.

For your information:

Pages : 149, 152-155

Exemption (b)(5) protects "inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency. Additionally, it protects deliberative process privilege."

Topics Covered

- DoDM 5240.01 Overview
- DoDM 5240.01 Procedures
  - Proc 2, Collection
  - Proc 3, Retention
  - Proc 4, Dissemination
  - Proc 5, Electronic Surveillance
  - Proc 6, Concealed Monitor
  - Proc 7, Physical Search
  - Proc 8, Mail Search/Cover
  - Proc 9, Physical Surveillance
  - Proc 10, Undisclosed Participation
- JA Checklist

Call Your Attorney

Primary POC
(b)(6),(b)(7)(C) **J.D., LL.M.**
Chief, National Security Law
(b)(6),(b)(7)(C)

NIPR: (b)(6),(b)(7)(C) **@us.af.mil**
SIPR: (b)(6),(b)(7)(C) **civ@mail.smil.mil**
JWICS: (b)(6),(b)(7)(C) **@af.ic.gov**

Alternate POC
Maj (b)(6),(b)(7)(C)
Deputy SJA
(b)(6),(b)(7)(C)

NIPR: (b)(6),(b)(7)(C) **1@us.af.mil**
SIPR: (b)(6),(b)(7)(C) **10.mil@mail.smil.mil**
JWICS: (b)(6),(b)(7)(C) **@af.ic.gov**

OSI/JA Main Line
(b)(6),(b)(7)(C)

THE AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS
FREEDOM OF INFORMATION ACT/PRIVACY ACT DELETED PAGE INFORMATION SHEET

5 pages withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Title 5, United States Code (U.S.C.), Section 552 (FOIA)				Title 5, U.S.C. Section 552a (PA)	
☐	(b)(1)	☐	(b)(7)(D)	☐	(d)(5)
☐	(b)(2)	☐	(b)(7)(E)	☐	(j)(2)
☐	(b)(3)	☐	(b)(7)(F)	☐	(k)(1)
☐	(b)(4)	☐	(b)(8)	☐	(k)(2)
☒	(b)(5)	☐	(b)(9)	☐	(k)(3)
☐	(b)(6)	☐		☐	(k)(4)
☐	(b)(7)(A)	☐		☐	(k)(5)
☐	(b)(7)(B)	☐		☐	(k)(6)
☐	(b)(7)(C)	☐		☐	(k)(7)

☐ Documents originated with (an)other Government agency(ies). These documents were referred to that agency for review and direct response to you.

____ pages contain information furnished by (an)other Government agency(ies). You will be advised by AFOSI as to the releasability of this information following our consultation with the other agency(ies).

____ pages have not been provided to you at this time because a final release determination has not been made. You will be advised as to the disposition at a later date.

For your information:

Pages : 149, 152-155

Exemption (b)(5) protects "inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency. Additionally, it protects deliberative process privilege."

Scenario

- You are stationed in Los Angeles, CA and tasked to surveil a military member suspected of providing classified information to a foreign power. You observe the member meeting with a known Chinese IO, driving a black Jeep Wrangler. While observing the meet you see a second individual, an unknown white male, with closely shaven hair approach the vehicle. In your reporting of the event can you:
  - Identify the primary subject?
  - Identify the Jeep Wrangler?
  - Describe the second individual?
  - What is the assumption of citizenship on the second individual?

Scenario

- You are grabbing a pint at Murphy's pub. You run into an old co-worker who is now an FBI agent. He states he heard you are working on a big Ukrainian FIS case. He wants to know if you can share information with him.

- Can you??

AFOSI and NCIS

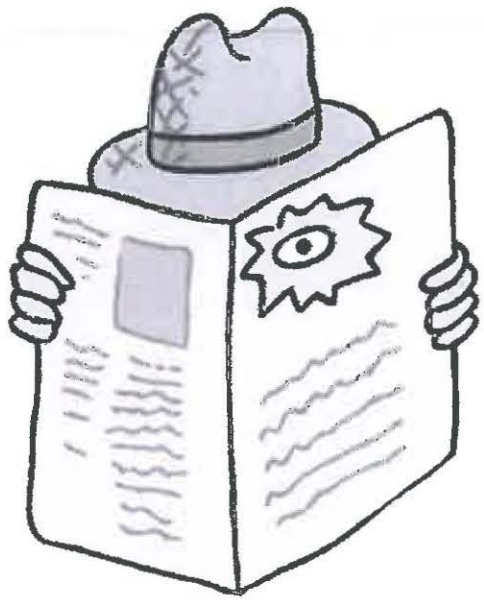
Legal Training for BCITP

U.S. AIR FORCE

January 2017

Points of Contact

- **NCIS**
  - (b)(6),(b)(7)(C)
  -
- **AFOSI**
  - (b)(6),(b)(7)(C)
  -



Agenda

- Significance of Executive Order 12333
  - Key Sections
  - History
  - Today
- Counterintelligence v. Law Enforcement
  - Definition
  - Assigned Missions (E.O. 12333)
- CI Jurisdiction and UCMJ
  - Personal and Subject Matter
  - Article 31(b)

Other relevant provisions of EO 12333

- E.O. 1.4—Role of the IC
  - Collect and provide information needed by the President
  - Collect information on int'l terrorism, proliferation of WMD
  - Analyze, produce, and disseminate intelligence
  - Conduct research, development, and procurement of technical systems and devices for the IC
  - Protect the security of intel related activities, information, installations, property, and employees
- E.O. 1.10—Roles of the DoD
  - The Secretary of Defense shall "collect (including through clandestine means), analyze, produce, and disseminate information and intelligence in response to tasking by the DNI and to execute SecDef's responsibilities

Our Mission per the President, E.O. 12333

- **E.O. 12333, 1.7(f) Intelligence Community Elements: ARMY, NAVY, AIR FORCE, AND USMC.**

- **The Commanders and heads of the intelligence and counterintelligence elements *shall*:**

  (1) Collect (including through clandestine means), produce, analyze and disseminate defense and defense-related intelligence and counterintelligence to support departmental requirements, and, as appropriate, national requirements;

  (2) Conduct counterintelligence activities;

  (3) Monitor the development, procurement, and management of tactical intelligence systems and equipment and conduct related research, development, and test and evaluation activities; and

  (4) Conduct military intelligence liaison relationships and military intelligence exchange programs with selected cooperative foreign defense establishments and international organizations

Counterintelligence Defined

Counterintelligence **means information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of *foreign powers*, organizations, or persons, or their agents, or *international terrorist organizations* or activities.**

-- EO 12333, 3.5(a)

What does the threat look like?

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

What are we up against?

Counterterrorism Defined

Counterterrorism is the activities and operations taken to neutralize terrorists and their organizations and networks in order to render them incapable of using violence to instill fear and coerce governments or societies to achieve their goals

-- Joint Publication 3-26 "Counterterrorism," 24 Oct 2014

- **FBI is lead for all CT cases in the US**

A Very Brief History . . .

- Spying is one of the oldest professions
  - General George Washington noted during the War of Independence "it was the British spies he feared the most."

- Today's laws and policies are the direct result of unfettered intelligence collection by DoD, FBI and CIA in the 1960s and 1970s.
  - Physical surveillance of public figures involved with the anti-Vietnam war and civil rights protests, e.g., MLK
  - Mail openings
  - Break-ins of the offices, vehicles and houses of U.S. persons
  - Undisclosed participation on university campuses

Unfettered Intelligence Collection

In September 1963, Attorney General Robert Kennedy gave permission to the FBI to break into Dr. Martin Luther King's home and install listening Devices.

The result?

- The Church and Pike congressional committees found the IC lacked policy on how to conduct it's mission in regards to U.S. persons
  - Recommended "reining" in Executive Branch powers in using intelligence elements against U.S. persons
  - Created the Permanent Select Committee on Intelligence (Senate) and the Congressional Committee on Intelligence
  - The Foreign Intelligence Surveillance Act was enacted in 1978

- Before Congress passed legislation to correct this deficiency, E.O. 11905 was signed, which was later replaced by E.O. 12333 (standing E.O. on Intelligence Oversight)

Current Concerns

- Continued desire of the U.S. government to ensure Intelligence Community personnel do not engage in activities which are illegal or that violate the rights of U.S. or other persons
  - Patriot Act renewal (renamed USA Freedom Act)
    - "The legislation we're considering proposes major changes to some of our nation's most fundamental and necessary counter-terrorism tools." Senate Majority Leader Mitch McConnell, R-Kent
  - DoDM 5240.01, 18 August 2016 -- NEW

- Areas of concern for the intelligence community:
  - Bulk data collection and databases
  - Insider Threat
    - Security Screening / Network Monitoring / Cyber activities
    - Mission Creep
  - Use of UAVs
  - The Internet
  - Others?

CI and LE Authorities

CI	LE
US Constitution Executive Order 12333 DoDM 5240.01 (Procs 1-10) DoD 5240.1-R (Procs 11-15) FISA (50 U.S.C. § § 1801 et seq) (National Security/Bank Letters) - 18 U.S.C. § 2709 (FBI only) - 15 U.S.C. § 1681v (DoD) - 12 U.S.C. § 3414 (FBI/DoD) - 50 U.S.C. § 3162 (FBI/DoD-travel records also available)	US Constitution DoDD 5200.27 - (U.S. Person) DoDI O-5505.09 - (Intercept Program) 18 U.S.C. § § 2701-2711 (ECPA-Electronic Communications Privacy Act) 18 U.S.C. § § 3121-27 (Pen/Trap Statute) 18 U.S.C. § § 2510-2522 (Wiretap Statute)

CI and Criminal Investigations

- Sister Services are inherently different (due to make-up and missions)
  - Army CI: Conducted solely by Intel professionals (No LE authority)
  - Navy CI: Conducted solely by NCIS Agents (dual CI/LE authorities)
  - AF CI: Conducted solely by AFOSI Agents (dual CI/LE authorities)
- USD(I) Policy controls CI investigations to include use of physical surveillance and other specialized collection techniques

Practice Points

- A CI investigation may transition to more LE methodology and techniques once charges are identified

- The approval authorities for some specialized collection techniques are lower for LE cases (physical surveillance and mail covers) and vice versa (oral wire intercepts)

Who can we investigate?

DoD CI Investigative Jurisdiction (of the Person)

CONUS

- **Active Duty Military**
- **Retired Military, Active or Inactive Reserve, Member of National Guard if suspected offense occurred when subject was in Title 10 status**

OCONUS

- **AD and DoD civilians and dependents**
- **DoD contractors or family members (Coor'd with CIA/FBI)**
- **Retired personnel and other foreign nationals (Coor'd with FBI/CIA)**

What can we investigate?

DoD CI Investigative Jurisdiction (subject matter)

- CI Investigative Jurisdiction (Subject Matter)
- Espionage, Treason, Spying, Subversion, Sedition
- FIS directed sabotage
- CI aspects of terrorism
- CI aspects of assassination or incapacitation of personnel
- Suicide/ AWOL of personnel with access/ clearance
- CI aspects of polygraph exams/ refusals
- CI aspects of unofficial travel or foreign contacts
- CI aspects of Insider Threat

Article 31(b), UCMJ

- Article 31(b) advice sounds a lot like Miranda except the military suspect is told what crime(s) they are suspected of committing.
- Also, military members receive the warnings, not only when they're in custody, but anytime they're officially questioned by someone who believes they have committed a criminal offense.
- Article 31(b) advice is an attempt to dispel the inherent compulsion a service member might feel to answer questions during interrogations by military superiors.

Taking a Moment....

Agenda, Part 2

- E.O. 12333
- DoDM 5240.01
  - Definitions (USPI, collection, retention and dissemination)
  - Procedure 2
  - Procedure 3
  - Procedure 4
  - Scenarios

Part II of EO 12333

"[T]o provide for the effective conduct of intelligence activities and the protection of constitutional rights...." -- EO 12333, Preamble

EO 12333, section 2.3

- Elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and *approved by the Attorney General*, consistent with the authorities provided by Part 1 of this Order, after consultation with the Director.

Who is a US Person?

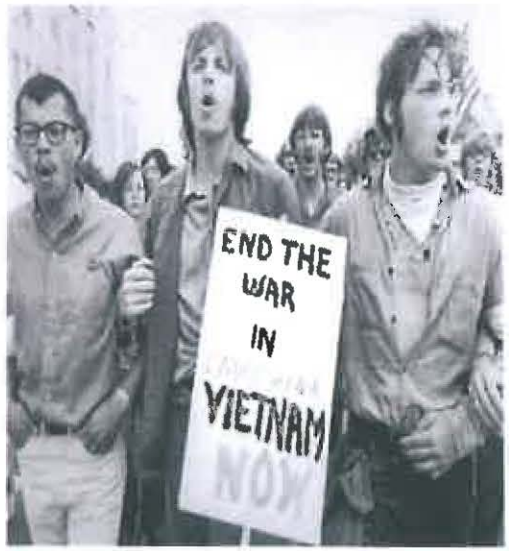
- US citizen
- Lawful permanent resident alien
- Unincorporated association substantially composed of US citizens or permanent resident aliens
- Corporation incorporated in the US, except for a corporation directed and controlled by a foreign government
- **NOTE:** A person or organization outside the US shall be presumed not to be a USP *unless specific information* to the contrary is obtained
- **Foreign national married to a U.S. servicemember?**

What is U.S. Person Information (USPI)?

- Information that is reasonably likely to identify one or more specific U.S. persons.
- May require a case-by-case assessment by a trained intelligence professional.
- May include names or unique titles; government-associated personal or corporate identification numbers; unique biometric records; financial information; and street address, telephone number, and Internet Protocol address info.
- Does not include:
  - A reference to a product by brand or manufacturer's name in a descriptive sense, e.g., Boeing 737

Basic Principles

- The rules permit CI investigations & operations targeting US persons, but must follow specific procedures
  - Do not infringe the constitutional rights of US persons
  - Protect privacy rights of persons entitled to protection
    - Rights to which a person is entitled depends on status and location
  - Perform a lawfully assigned function
  - Employ least intrusive techniques
    - If conducted in the US or directed against a US person
  - Comply with regulatory requirements
    - Review and approval requirements



Okay, but how can we do it?

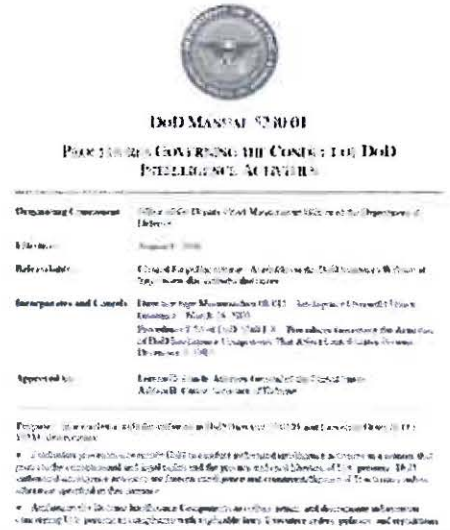
- **DoDM 5240.01 and DoD 5240.1-R apply to activities of DoD Intelligence Components**

  DoDM 5240.01 (8 Aug 2016)

  - **Procedures 2 - 4: Authority to collect, retain, and disseminate United States person information (USPI)**
  - **Procedures 5 - 10: Guidance for *specialized* techniques to collect foreign intelligence and counterintelligence**

  DoD 5240.01-R (7 Dec 1982)

  - **Procedures 11 - 15 govern other aspects of DoD intel activities, including the oversight of such activities.**



DoD MANUAL 5240.01

PROCEDURES GOVERNING THE CONDUCT OF DoD INTELLIGENCE ACTIVITIES

Procedure 2, Collection of USPERS Info

- Rule 1: You may intentionally collect USPI only if the information sought is *reasonably believed* to be *necessary* for the performance of an authorized intelligence mission or function, and if the USPI falls within one of the 13 categories

- Collection = Information is collected when it is *received* whether or not it is retained for intelligence or other purposes.
  - Regardless of when you use it
  - Computers can collect
  - Intel is collected only once

- Must use LEAST INTRUSIVE MEANS as are practicable when collecting USPI

Procedure 2, Reasonable Belief

- When the facts and circumstances are such that a reasonable person would hold the belief.
- Must rest on facts and circumstances that can be articulated
- Hunches or intuitions are not sufficient.
- Can be based on experience, training, and knowledge of foreign intelligence or CI activities as applied to particular facts and circumstances.

Procedure 2, 13 Collection Categories

1. Publicly Available
2. Consent
3. Foreign Intelligence (FI)
4. Counterintelligence (CI)
5. Threats to Safety
6. Protection of Sources/Methods
7. Current, Former, or Potential Sources
8. Persons in Contact With Sources or Potential Sources
9. Personnel Security
10. Physical Security
11. Communications Security
12. Overhead and Airborne Reconnaissance
13. Administrative Purposes

Procedure 2, 13 Collection Categories

1. **Publicly Available**
   - Not the same as OSINT

2. **Consent**
   - Implied consent: The legal advisor will determine whether a notice or policy is adequate and lawful, before the Component takes or refrains from taking action on the basis of implied consent.

3. **Foreign Intelligence**
   - (a) An individual reasonably believed to be an officer or employee of, or otherwise acting on behalf of, a foreign power;
   - (b) An organization or group reasonably believed to be directly or indirectly owned or controlled by, or acting on behalf of, a foreign power;
   - (c) An individual, organization, or group reasonably believed to be engaged in or preparing to engage in international terrorist or international narcotics activities;
   - (d) An individual, organization, or group who is a target, hostage, or victim of an international terrorist or international narcotics organization.

Procedure 2, 13 Collection Categories

4. Counterintelligence

- The information is *reasonably believed* to constitute CI and the U.S. person is one of the following:

(a) An individual, organization, or group reasonably believed to be engaged in or preparing to engage in espionage, other intelligence activities, sabotage, or assassination on behalf of a *foreign* power, organization, or person, or on behalf of an agent of a *foreign* power, organization, or person;

(b) An individual, organization, or group reasonably believed to be engaged in or preparing to engage in international terrorist activities;

(c) An individual, organization, or group reasonably believed to be acting for, or in furtherance of, the goals or objectives of an international terrorist or international terrorist organization, for purposes harmful to the national security of the United States; or

(d) An individual, organization, or group *in contact with a person described above* for the purpose of identifying such individual, organization, or group and assessing any relationship with the person described therein.

Procedure 2, 13 Collection Categories

5. **Threats to Safety**
   - Information needed to protect the safety of any person or organization, including those who are targets, victims, or hostages of international terrorist organizations, if:
     (a) The threat has a *foreign* connection;
     (b) Component head or delegee has determined that a person's life or physical safety is *reasonably believed* to be in imminent danger; *or*
     (c) The information is needed to maintain maritime or aeronautical safety of navigation.

6. **Protection of Intelligence Sources, Methods, and Activities**
   - The information is about U.S. persons who have access to, had access to, will have access to, or are otherwise in possession of information that reveals foreign intelligence or CI sources, methods, or activities, when collection is reasonably believed necessary to protect against the unauthorized disclosure of such information.

Procedure 2, 13 Collection Categories

7. Current, Former, or Potential Sources of Assistance

- The information is about those who are or have been sources of information or assistance, or are reasonably believed to be potential sources of information or assistance, to intelligence activities for the purpose of assessing their suitability or credibility.

8. Persons in Contact with Sources or Potential Sources

- The information is about persons in contact with sources or potential sources, for the purpose of assessing the suitability or credibility of such sources or potential sources.

9. Personnel Security

- The information is arising from a lawful personnel security investigation.

10. Physical Security

- The information is about U.S. persons reasonably believed to have a *foreign* connection and who pose a threat to the physical security of DoD personnel, installations, operations, or visitors
- Must have or be supporting an authorized physical security mission and must be able to articulate a reasonable belief in both the foreign connection of the U.S. persons who are collection targets and the physical security threat they pose

Procedure 2, 13 Collection Categories

11. Communications Security Investigation

- The information is arising from a lawful communications security investigation

12. Overhead and Airborne Reconnaissance

- May intentionally collect imagery that contains USPI provided that the collection is ***not*** directed at a specific U.S. person or, if the collection is directed at a specific U.S. person, the collection falls in one of the other 12 categories
- Includes information obtained from unmanned aircraft systems

13. Administrative Purposes

Procedure 2, Least Intrusive Means

- **Least Intrusive Means**
  - **Use the least intrusive collection techniques feasible within the United States or when directed against a U.S. person abroad.**
    - **Publicly available sources or with the consent of the person concerned**
    - **Cooperating sources**
    - **Techniques that do not require a judicial warrant or AG approval**
    - **Techniques that do require a judicial warrant or AG approval**

Procedure 2, Other

- Special Circumstances Collection – BIG DATA
  - Defense Intelligence Components ***will*** consider whether collection opportunities raise special circumstances based on the volume, proportion, and sensitivity of the USPI likely to be acquired, and the intrusiveness of the methods used to collect the information

- Amount of Information Collected
  - In collecting non-publicly available USPI, to the extent ***practicable***, collect no more information than is reasonably necessary

Threshold Questions

- Are we collecting?
- Does the collection concern USPI?
- Does the collection fall within assigned mission/ function?
- Does the information collected fall within one of the 13 permissible categories?
- Are you using the least intrusive method?

- Consider the following collection "formula":

Mission + Reasonable Basis + Procedure = Collection

Procedure 3, Retention

- Permanent retention standard
  - Retention is reasonably believed to be necessary for the performance of an authorized intelligence mission; and
  - The information was lawfully collected or disseminated to the Component
    - Meets one of the 13 collection categories; or
    - Is necessary to understand or assess CI, e.g., information about a U.S. person that provides important background or context for CI.

Procedure 3, Retention

- Three primary evaluation periods to determine permanent retention of USPI
  - Promptly
  - Five (5) years
  - Twenty-five (25) years

- Intentional Collection of USPI
  - Must be evaluated promptly; and
  - If *necessary*, may retain the information for evaluation for up to 5 years, subject to extension

Procedure 3, Retention

- **Incidental Collection of USPI**
  - Defined: collection of USPI that is not deliberately sought, but is nonetheless collected
  - *Person in the United States,* may retain all of the incidentally collected information for evaluation for up to 5 years, unless extended
  - *Person outside the United States, may* retain all of the incidentally collected information for evaluation for up to 25 years

- **Voluntarily Provided USPI**
  - About a U.S. person, evaluate the information promptly, up to 5 years, unless extended.
  - About a non-U.S. person, evaluation for up to 25 years

Procedure 3, Retention

- **Unintelligible information**
  - The time periods begin when the information is processed into intelligible form
  - Includes information that a Component cannot decrypt or understand in the original format.
  - To the extent practicable, unintelligible information will be processed into an intelligible form.
  - Text in a foreign language is considered intelligible

- **Deletion of information**
  - Unless the standards for permanent retention are met, ***must*** delete all USPI from the Component's automated systems of records

Procedure 4, Dissemination

- We may disseminate USPI based upon the following criteria:
  - Any person or entity: Information is publicly available or U.S. person has consented to the dissemination.
  - Other intelligence community elements
  - Other DoD elements; federal government entities; state, local, tribal, or territorial governments: recipient is reasonably believed to have a need to receive such information for the performance of its lawful missions or functions.
  - Foreign governments or international organizations
    - Recipient is reasonably believed to have a need to receive such information for its lawful missions or functions; and
    - Disclosure is consistent with applicable international agreements and foreign disclosure policy
  - Protective Purposes: Necessary to protect the safety or security of persons or property, or to protect against or prevent a crime or threat to the national security

Questions on Procedures 2 – 4?

BREAK TIME

Agenda, Part 3

- Special Collection Procedures
  - Procedure 5 – Electronic Surveillance
  - Procedure 6 – Concealed Monitoring
  - Procedure 7 – Physical Search
  - Procedure 8 – Mail Covers
  - Procedure 9 – Physical Surveillance
  - Procedure 10 – Undisclosed Participation

Procedure 5, Electronic Surveillance

- Implements FISA and E.O. 12333
- Defined
  - The installation or use of any monitoring device in the United States where a person has a reasonable expectation of privacy, as determined by the legal advisor, and
  - A warrant would be required for law enforcement purposes.
- Fourth Amendment
  - All electronic surveillance must comply with the Fourth Amendment
  - The legal advisor is required to assess the reasonableness of collection, retention, and dissemination

Reasonable Expectation of Privacy

- Reasonable expectation of privacy (REP)
  - Can a person have a REP in a government office?
  - REP if a person has a private office with locked door?
  - Does a person in a public street ordinarily have a REP?
  - A person in their vehicle on public roads? A private garage?
- Generally, no expectation of privacy in . . .
  - Bank records (NSL)
  - Public activities
  - Garbage left at the curb, abandoned property
  - Handwriting
  - Smell of luggage
- Legal advisor needs the facts from the field re: REP

Procedure 5, Electronic Surveillance

- In the United States:
  - Attorney General or the Foreign Intelligence Surveillance Court (FISC) may authorize, except for emergency situations
  - May only conduct such surveillance if both:
    - A significant purpose of the electronic surveillance is to obtain foreign intelligence information; and
    - There is probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power

Procedure 5, Electronic Surveillance

- **Outside the United States:**
  - U.S. person
    - Governed by FISA and E.O. 12333; or
    - Approval under exigent circumstances exception
  - Non-U.S. person: governed by Title I or Section 702
- **Emergency situations: Attorney General approval**

- **Technical Surveillance Countermeasures (TSCM)**
  - Applies to the use of electronic equipment and specialized techniques to determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance

FISA

- Ensure you are written into the FISA request:
  - Make sure your personnel are authorized, within the request to receive FISA info, and that your equipment is authorized to be used as part of FISA collection.
- Dissemination of FISA derived information must include the caveat that use in any criminal proceeding requires prior approval from the AG.

Procedure 6, Concealed Monitoring

- Defined as the following:
  - Hidden electronic, optical, or mechanical devices,
  - to monitor a particular person or a group of persons,
  - without consent,
  - in a surreptitious manner,
  - over a period of time, and
  - no reasonable expectation of privacy

- Examples
  - Video monitoring or sound recording of a subject in a place where he or she has no reasonable expectation of privacy if conducted over a period of time
  - Taking one photograph of a subject would not qualify

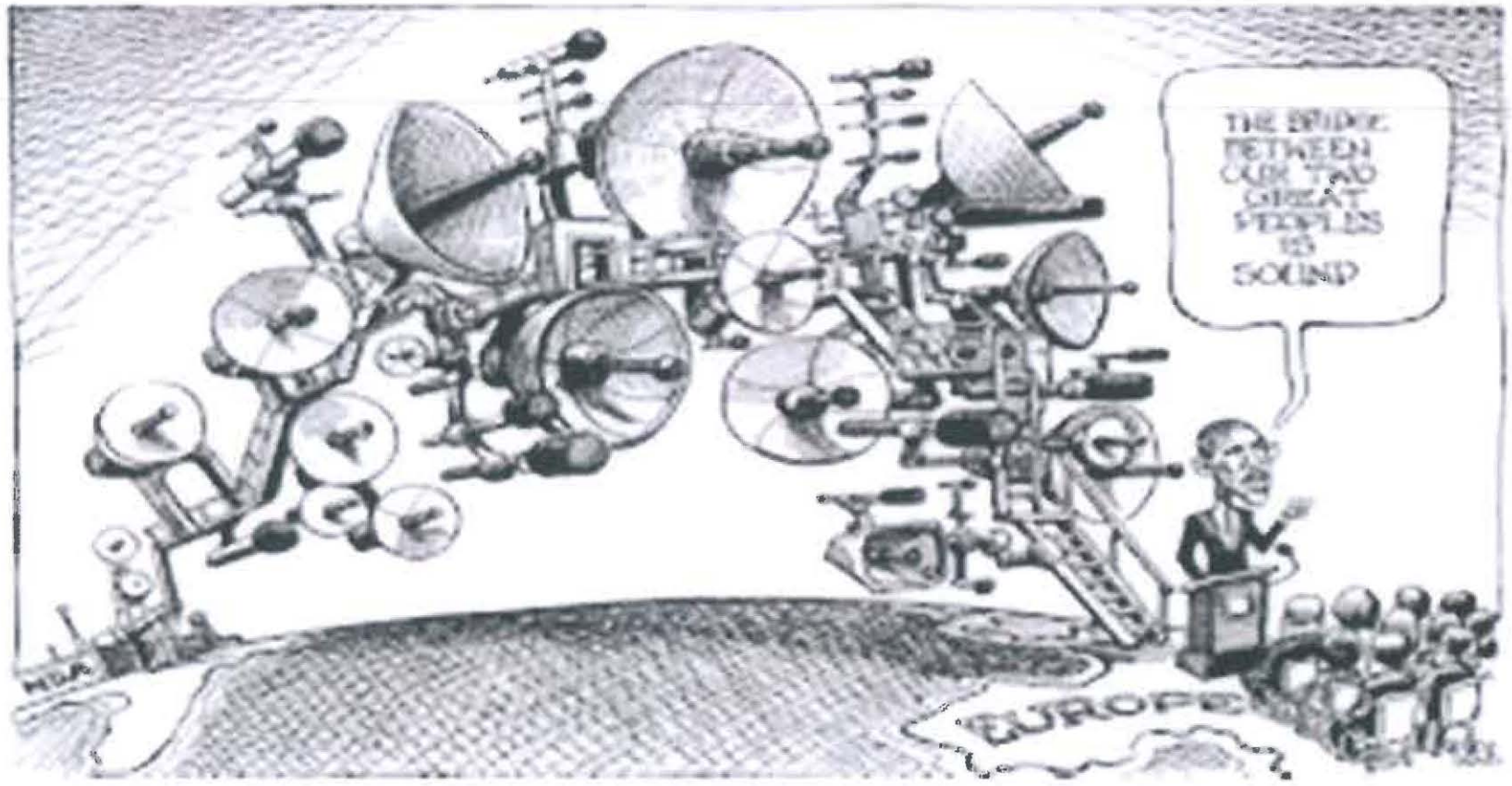
Procedure 6, Concealed Monitoring

- Scope: Proc 6 applies to the following:
  - Any person inside the United States, and
  - Any U.S. person outside the United States
- With the appropriate approval and coordination, we may conduct concealed monitoring . . .
  - In the United States
    - On DoD facilities
    - Outside DoD facilities after coordination with the FBI
  - Outside the United States
    - On DoD facilities
    - Outside DoD facilities must be coordinated with the CIA, and appropriate host country officials in accordance with any applicable SOFA or other international agreement

Procedure 6, Concealed Monitoring

- Approval: Component head or delegee
- Component legal is required to determine whether the following criteria have been met:
  - There is no reasonable expectation of privacy;
  - Such monitoring is necessary to conduct an assigned CI function;
  - A trespass will not be necessary to effect the monitoring; and
  - The monitoring is not subject to Procedure 5
- For more on trespass, see U.S. v. Jones, Sup. Ct. (2012)
  - Physical attachment of GPS tracking device on vehicle to monitor its movement is a trespass/search under Fourth Amendment

Taking a Moment...



Procedure 7, Physical Searches

- Scope: Applies to *nonconsensual* physical searches in the United States *and* of U.S. persons/property outside the United States
- Defined: Any intrusion on a person or property that would require a *warrant* for law enforcement purposes
- Does *not* include examinations of the following:
  - Areas that are in plain view and visible to the unaided eye if there is no physical trespass;
  - Publicly available information;
  - Abandoned property in a public place;
  - Items where we have consent; and
  - Government property pursuant to Military Rule of Evidence 314(d)

Procedure 7, Physical Searches

- **Approval Required**
  - Search of active duty: Attorney General or Foreign Intelligence Surveillance Court
  - Search of other persons inside the United States
    - We may NOT conduct searches of other persons in the U.S.
    - We may request the FBI to conduct such searches
  - Other U.S. persons outside the United States
    - The search is for an authorized CI purpose;
    - The search is appropriately coordinated with the CIA; and
    - The FISC or the Attorney General has authorized the search.
    - Who may request: SecDef, DSD, USD(I); SecAF; USecAF; DIRNSA/CHCSS; Director, DIA; Director, NGA; or Director, NRO

Procedure 8, Mail Searches and Cover

- **Mail Searches**
  - See Procedure 7

- **Mail cover, e.g., examination of envelope**
  - In U.S. postal service channels, request the USPS IAW 39 CFR 233.3(e)(2)
  - In foreign postal channels, may request a mail cover for mail that is to or from a U.S. person consistent foreign law and any applicable SOFA

Procedure 8, Mail Searches and Cover

- Any National Security mail cover request must be approved personally by the head of the law enforcement agency or intelligence component requesting the cover or the one designee at the agency's headquarters
- Original signed copy is forwarded to Chief Postal Inspector
- Postal has cleared facilities, request/justification must be specific to case details

Procedure 9, Physical Surveillance

- **Who can we surveil in the United States:**
  - Military service members;
  - Present or former military or civilian employees of a DIC;
  - Present or former contractors of a DIC;
  - Present or former employees of such a contractor;
  - Applicants for such employment or contracting;
  - Non-U.S. persons; and
  - Other persons, "when detailed to the FBI or when operating under FBI authorities."

Procedure 9, Physical Surveillance

- **Scope**
  - Any person inside the United States or any U.S. person outside the United States
  - Applies to any devices used to observe the subject of the surveillance (not Procedure 6)

- **Defined**
  - Deliberate and continuous observation of a person, and
  - Where the person has no reasonable expectation of privacy
  - Does <u>not</u> apply to surveillance detection or counter surveillance used to detect and elude foreign physical surveillance

DoD Intelligence Components

- NSA
- DIA
- The offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs.
- The Assistant Chief of Staff for Intelligence, Army General Staff.
- The Office of Naval Intelligence.
- The Assistant Chief of Staff, Intelligence, U. S. Air Force.
- The Army Intelligence and Security Command.
- The Naval Intelligence Command.
- The Naval Security Group Command.
- The Director of Intelligence, U.S. Marine Corps.
- The Air Force Intelligence Service.
- The Electronic Security Command, U.S. Air Force.
- The counterintelligence elements of the Naval Investigative Service.
- The counterintelligence elements of the Air Force Office of Special Investigations.
- The 650th Military Intelligence Group, SHAPE.
- Other organizations, staffs, and offices, when used for foreign intelligence or counterintelligence activities to which part 2 of E.O. 12333 (reference (a)), applies, provided that the heads of such organizations, staffs, and offices shall not be considered as heads of DoD intelligence components for purposes of this Regulation.

Procedure 9, Physical Surveillance

- **Approval and coordination**
  - **Approval: Component head or delegee**
  - **Coordination**
    - **In the United States**
      - No coord req'd for on-base surveillance of active duty
      - FBI coord for all off-base surveillance
      - FBI coord for on-base surveillance of non-active duty
    - **Outside the United States**
      - CIA for off-base surveillance
      - Consider with SOFA and foreign law/policy

Procedure 10, Undisclosed Participation

- Scope: Governs the participation by DICs and anyone acting on behalf of a DIC, e.g., sources, in any organization in the United States or any organization outside the United States that constitutes a U.S. person.
- Organization defined
  - An association of two or more individuals formed for any lawful purpose whose existence is formalized in some manner
  - Includes those that meet and communicate through the use of technologies
- Participation defined
  - When a person is tasked or asked to participate in an organization for the benefit of the DIC
  - Actions undertaken "for the benefit of" a DIC may include collecting information, identifying potential sources or contacts, or establishing or maintaining cover.

Procedure 10, Undisclosed Participation

- Exclusions
  - Personal participation
  - Voluntarily provided information
  - Publicly available information on the Internet
    - Collection of publicly available information on the Internet in a way that does not require a person to provide identifying information (such as an email address) as a condition of access and does not involve communication with a human being

- Approval level depends on the activity—see below
  - No specific level of approval (NOT no approval)
  - Component head or delegee
  - Component head or single delegee

Procedure 10, Undisclosed Participation

- UDP requiring no specific level of approval
  - Education or training
  - Cover Activities: Participation in an organization solely for the purpose of obtaining or renewing membership status *in accordance with DoD cover policy*
  - Published or posted information: Participation in an organization whose membership is open to the public solely for the purpose of obtaining information published or posted by the organization or its members and generally available to members; must not involve elicitation.
  - Public forums: Employment affiliation not req'd and no elicitation of USPI; and
  - Foreign entity: Participation in an organization that is an entity openly acknowledged by a foreign government to be directed or operated by that foreign government or is reasonably believed to be acting on behalf of a foreign power, and the organization is reasonably believed to consist primarily of individuals who are non-U.S. persons.

Procedure 10, Undisclosed Participation

- UDP That May Be Approved by a component head or delegee
  - Non-U.S. persons as potential sources of assistance
  - Public forums: employment affiliation required or elicitation of USPI may be authorized
  - Cover activities: beyond obtaining or renewing membership for the purpose of maintaining or enhancing cover
  - U.S. person organizations outside the United States: involving participation from or about a non-U.S. person located outside the United States

Procedure 10, Undisclosed Participation

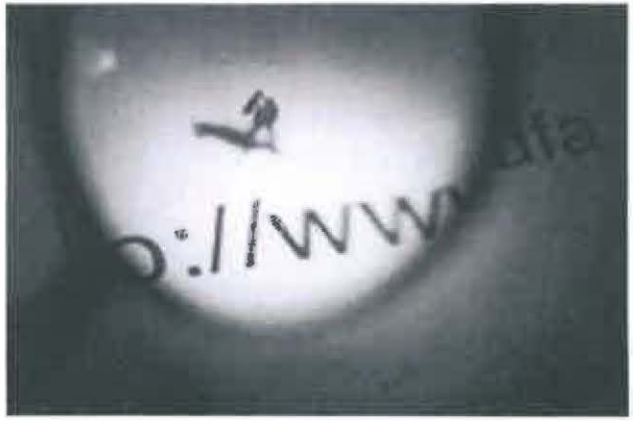
- **UDP That May Be Approved by a Defense Intelligence Component Head or a Single Delegee**
  - To conduct authorized CI activities not otherwise addressed in or outside the United States, after required coordination with the FBI or CIA.
  - To collect information inside the United States necessary to identify a U.S. person as a potential source of assistance to foreign intelligence or CI activities.
  - To collect information outside the United States necessary to assess a U.S. person as a potential source of assistance to foreign intelligence or CI activities

Procedure 10, Undisclosed Participation

- **Standards for review and approval: approving official must make the following determinations:**
  - **The potential benefits to national security outweigh any adverse impact on civil liberties or privacy of U.S. persons**
  - **The proposed UDP complies with the limitations on UDP; and**
  - **The proposed UDP is the least intrusive means feasible and conforms to the requirements of Procedure 2**

UDP Online/ Social Networking Sites

- Undisclosed Participation is applicable in the CYBER world…
- Is the website an organization/USP? Look to facts:
  - Primarily US users
  - Location of the server
  - Incorporation
  - Website content
  - Language used
  - Richard Shriffin memo
- Other matters
  - Cover Plan?
  - De-confliction?



Take a Moment . . .
(for our LE friends)

Agenda, Part 4

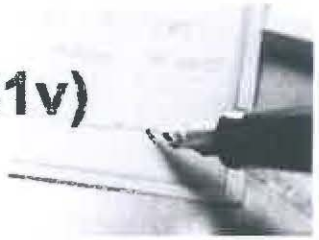
- Additional Legal Authorities / Special Collection
  - Bank and National Security Letters
    - Right to Financial Privacy Act (12 USC §3401)
    - Fair Credit Reporting Act (15 USC §1681(v))
    - Requests by Authorized Investigative Agencies (50 §USC 3162)
    - FBI Request for Telephone Toll and Transactional Records (18 USC §2709)
  - DoD IG Subpoena
  - Electronic Communications Privacy Act (ECPA), 18 USC §2701
  - Computer Trespasser Exception, 18 USC §2511(2)(i)

National Security Letters (NSLs)

- Several Federal statutes authorize intelligence officials to request certain business record information in connection with national security investigations.
- Prospects of continued NSL use is dimming
- What Congress gives, Congress can take away, but for now…..

Summary: Types of NSLs

- Financial Information - Bank Letter (12 USC 3414)
  - Non-compulsory for DoD
    - FBI has authority to compel per para (a)(5)(A)
- Credit Reporting Agency Letter (15 USC 1681v)
  - Compulsory
  - International terrorism only
- Security Clearance Investigations (50 USC 3162)
  - Requires consent; check SF 86 Paperwork!
  - Gets you Bank Records, Credit Reports and Travel Records
  - Compulsory
- Telephone and Toll Records/ISP (18 USC 2709)
  - Available only to the FBI



NSL - Bank Letter, 12 USC § 3414

- What type of records?
  - Any record held by a financial institution pertaining to a customer's relationship with the financial institution
  - Customer need not be the target of the investigation
  - Financial institutions broadly defined

NSL - Bank Letter, 12 USC § 3414

From whom can we request?

- Bank
- Savings bank card issuer
- Industrial loan company
- Trust company
- Savings association
- Building and loan, or homestead association (including cooperative banks)
- Credit union
- Consumer finance institution
- Broker registered w/ SEC

- Pawn broker
- Insurance Company
- U.S. Postal Service
- Dealer in jewels and precious stones
- Travel Agency
- Vehicle sales
- Casinos
- Persons involved w/ real estate closings

NSL - Credit Reporting Agency, 15 USC §1681v

- What type of records?
  - Customer credit reports and all other customer records
- Who can we compel to provide?
  - Consumer Reporting Agencies

EQUIFAX

experian

TransUnion

- When?
  - Must be related to International Terrorism

NSL - Security Clearance Investigations, 50 USC § 3162

- What type of records?
  - Financial records
  - Records pertaining to travel outside the U.S.

- Who can we request from?
  - Financial Institutions
  - Credit reporting agencies
  - Commercial entities within the U.S. with records refl travel outside the U.S.

NSL - Security Clearance Investigations, 50 USC § 3162

- TARGET
  - Executive Branch Employee
  - Who as *a condition of access to classified information*
  - Provided consent (during background investigation)
  - for a period of not more than 3 years thereafter to financial and travel records;

AND

Reasonable grounds to believe that the target

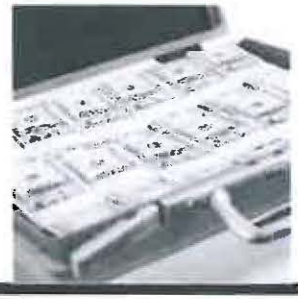
- is or may be disclosing classified info in an unauthorized manner to a foreign power or agent of a foreign power

Or

- has incurred excessive indebtedness or has acquired a level of affluence which cannot be explained by other info;

Or

- had the capability and opportunity to disclose classified info which is known to have been lost or compromised to a foreign power or agent of a foreign power



NSL Summary Chart

Profile of the Current NSL Statutes

NSL Statute	18 U.S.C. 2709	12 U.S.C. 3414	15 U.S.C. 1681u	15 U.S.C. 1681v	50 U.S.C. 3162
Addressee	communications providers	financial institutions	consumer credit agencies	consumer credit agencies	financial institutions, consumer credit agencies, travel agencies
Certifying officials	senior FBI officials and SACs	senior FBI officials and SACs; or supervisory official of a rank designated by the head of the investigating agency	senior FBI officials and SACs	supervisory official of an agency investigating, conducting intelligence activities relating to or analyzing int'l terrorism	senior officials no lower than Ass't Secretary or Ass't Director of agency w/ employees w/ access to classified material
Information covered	identified customer's name, address, length of service, and billing info	identified customer financial records	identified consumer's name, address, former address, place and former place of employment	consumer report and all other information in a consumer's file	all financial information and foreign travel records relating to consenting employee
Standard/ purpose	relevant to an investigation to protect against int'l terrorism or clandestine intelligence activities	sought for foreign counterintelligence purposes to protect against int'l terrorism or clandestine intelligence activities	sought for an investigation to protect against int'l terrorism or clandestine intelligence activities	necessary for the agency's investigation, activities, or analysis of int'l terrorism	necessary to conduct a law enforcement investigation, CI inquiry or security determination

DoD IG Subpoena

- DoD IG Subpoenas may be used to Support Non-Fraud related investigations when
  - There is sufficient DoD nexus to the crime at issue to warrant the DoD IG's involvement in the investigation
    - Meaning (1) Agency must have investigative authority for the crime under investigation and (2) if the investigation is being conducted jointly the DoD entity must be designated the "lead investigative organization" and
  - The particular crime at issue of such a nature and/or such concern to DoD as to warrant the DoD IG's involvement in the investigation
    - Terrorism, Espionage, Agent for Foreign Government, Spies, Aiding the enemy are among the 25 delineated crimes

DoD IG Subpoena

- Documents and instructions available on DoD IG Website at

http://www.dodig.mil/Programs/Subpoena/subpoena.html

Mechanisms for Acquiring ISP data

- Request FBI pursue an NSL for Telephone Toll and Transactional Records, IAW 18 USC 2709
  - This option is NOT available to DoD entities in unilateral cases
  - Provides Subscriber Data and toll billing records, along with electronic comm transactional records




- 18 USC 2703 offers several mechanisms that a government entity may use to compel disclosure

Electronic Communications Privacy Act (ECPA)

- BLUF: USGOV can't access emails, data logs or subscriber data with nothing in hand
- ECPA governs information stored on Public Internet Service Providers (ISPs) and on Public Networks
  - Fewer requirements for private networks, such as DoD's
  - Plus, we obtain consent through Banner/User Agreement/IA Training
- General rule for ECPA: it is unlawful to access, obtain, alter or prevent access to wire or electronic communications while in storage by a provider of such communications services

ECPA Summary Chart

Preservation Letters

- If contemplating action under ECPA the first step is to PRESERVE the stored comms/data
- Requirement to preserve records or evidence in the ISP's possession pending the issuance of court order or other process for 90 days (additional 90 day extension is available) per 18 USC 2703(f)
- How to identify the ISP POC:
  - http://www.copyright.gov/onlinesp/list/a_agents.html (Service Provider's agents for notification of claims of copyright infringement)
  - http://www.search.org/resources/isp-list/

Computer Trespasser Exception, 18 USC §2511(2)(i)

- **Live monitoring of Internet/network communication is lawful provided the four (4) criteria are met:**
  - **1. The owner or operator of the protected computer must authorize the interception of a trespasser's communications.**
  - **2. The person intercepting the communication must be lawfully engaged in an ongoing investigation.**
  - **3. The person intercepting the communication must have reasonable grounds to believe that the contents of the communications to be intercepted will be relevant to the ongoing investigation.**
  - **4. The monitoring must be configured so that it only intercepts the trespasser's communications.**

Taking a moment...

Agenda

- Material Support to Terrorism (MST) Statutes (18 USC §§ 2339A and 2339B)
- Protection of Defense Information
  - 18 USC §793 - 18 USC §798
  - 18 U.S.C. §1924
  - Classification Reviews and CIPA
- Sanctions
  - TWEA and IEEPA (Dept of Treasury)
- Export Control
  - International Traffic in Arms Regulations (Dept of State)
  - Office of Foreign Assets and Control (Dept of Commerce)

Material Support to Terrorists (MST) Statutes

- "Material support" includes almost any kind of support for blacklisted groups; including humanitarian aid, training, expert advice, "services" in almost any form, and political advocacy.
  - Intent to further the illegal activities of the terrorist organization (presumption that any contribution to a terrorist organization furthers or facilitates criminal activity)

- 18 USC § 2339A Providing material support to terrorists
- 18 U.S.C. § 2339B Providing material support to designated foreign terrorist organizations

MST Applicability to You

- The term "whoever" within the statute and legislative history includes "government actors"
  - Ensure you and your assets are covered!
  - This can be a timely approval process so plan accordingly

- Each Agency has its own
  - Approval policy
    - Lethal Aide
  - Coordination with DOJ

Protection of Defense Information (18 USC 793-798)

- It all started with the Espionage Act of 1917
  - It originally prohibited any attempt to interfere with military operations, to support U.S. enemies during wartime, to promote insubordination in the military, or to interfere with military recruitment.
  - Passed along with the Trading with the Enemy Act
  - Espionage Act was based on the Defense Secrets Act of 1911, especially the notions of obtaining or delivering information relating to "national defense" to a person who was not "entitled to have it"

Statutes

- 18 USC § 793 - Gathering, transmitting or losing defense information
- 18 USC § 794 - Gathering or delivering defense information to aid foreign government
- 18 USC § 795 - Photographing and sketching defense installations
- 18 USC § 796 - Use of aircraft for photographing defense installations
- 18 USC § 797 - Publication and sale of photographs of defense installations
- 18 USC § 798 - Disclosure of classified information

Use of Classified Information in Court

- For these types of cases you will need the compromised information reviewed for an evaluation of harm to national defense if released and approval for use in charging/ trial
  - This will be a timely and occasionally an "emotional" experience
  - Prior to 2015, DoJ was requiring SECRET or above to charge
- Classified Information Protection Act (CIPA) and MRE Rule 505 provide for protection of the classified information during court proceedings
- False Flag Operations

Sanctions and Export Controls

- The principal statutes underpinning U.S. sanctions and embargos are administered by the Department of the Treasury:
  - The Trading With the Enemy Act (TWEA)
  - International Emergency Economic Powers Act (IEEPA)

These sanctions are further codified by:

- Office of Foreign Assets and Control (Department of Commerce)
- Arms Export Control Act via International Traffic in Arms Regulations (Department of State)

Sanctions: IEEPA (50 USC §§1701-1707)

- Authorizes the POTUS to regulate commerce with certain persons/countries after declaring a national emergency in response to an unusual and extraordinary threat from a foreign source.
  - Country or designated nationals list
  - Non-Proliferation Sanctions
  - Counter Terrorism Sanctions
  - Counter Narcotic Sanctions
  - Transnational Criminal Orgs

- Administered by Dep't of Treasury
- Restrictions apply to all U.S. persons and entities…

Sanctions: Office of Foreign Assets and Control (OFAC)

- OFAC administers a number of different sanctions programs. The sanctions can be either comprehensive or selective, using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals
- OFAC oversees, imposes penalties pursuant to, and grants licenses to permit activities covered by U.S. sanctions.
- Fines for violations: $50K to $100K and imprisonment from 10 to 30 yrs for willful violations.

OFAC Licenses

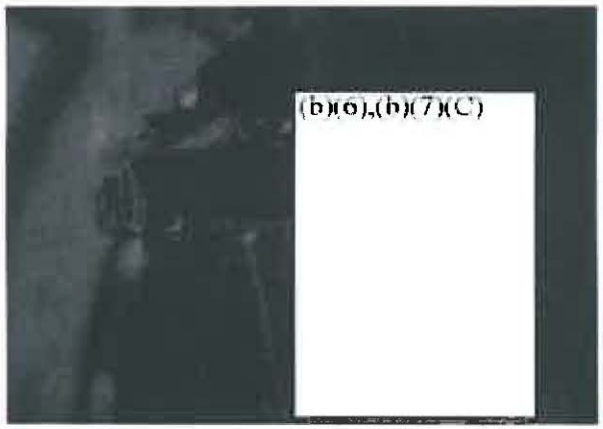
- There are two types of licenses:
  - A general license authorizes a particular type of transaction for a class of persons without the need to apply for a license.
  - A specific license is a written document issued by OFAC to a particular person or entity, authorizing a particular transaction in response to a written license application.
- Persons engaging in transactions pursuant to general or specific licenses must make sure that all conditions of the licenses are strictly observed.

Arms Export Control Act (Inter'l Traffic in Arms Regs)

- Administered by the Department of State
- 22 USC §2778 of the Arms Export Control Act (AECA) provides the authority to control the export of defense articles and services
- Executive Order 11958, as amended, delegated this statutory authority to the Secretary of State.
- International Traffic in Arms Regs (ITAR) implements this authority

ITAR (22 USC §2778)

- All U.S. manufacturers, exporters, and brokers of defense articles, defense services, or related technical data, as defined on the USML, are required to register with U.S. Department of State
- A foreign person is any person who is not a lawful permanent resident of the U.S. and includes foreign governments and organizations



ITAR Exceptions

- ITAR does not apply to information related to general scientific, mathematical or engineering principles that is commonly taught in schools and colleges or information that is (legitimately) in the public domain
- Each agency has own procedures and approvals for dealing with ITAR controlled items.

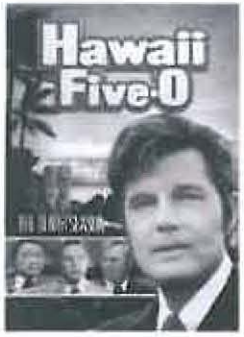


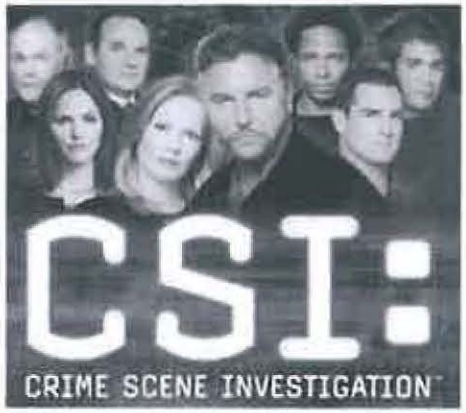
One last chance to meet your attorneys!

- NCIS
  - (b)(6),(b)(7)(C)
  -
  -
- AFOSI
  - (b)(6),(b)(7)(C)
  -
  -

Questions?

MARINES
THE FEW THE PROUD





GPS Trackers and Transponders

- U.S. v. Jones, January 2012 Supreme Court Ruling
- Physical attachment of GPS tracking device to monitor a vehicle is a trespass/ search
- Result for DoD?
  - Must use FISA or Procedure 7 –
  - Physical search authority
  - You will need to be able to
  - provide probable cause…