Defense Security Service
Intelligence Oversight Awareness
Training Course
Transcript for Non-CI

Welcome

In a 2013 testimony to congress on Foreign Intelligence Surveillance, the former Director of National Intelligence, LT GEN James Clapper (Ret), spoke about limitations to intelligence activities as pertaining to US persons.

LT GEN James Clapper (Ret): “This public discussion should be based on an accurate understanding of the Intelligence Community; who we are, what we do, and how we are overseeing it. In the last few months the manner in which are activities have been characterized has often been incomplete, inaccurate, or misleading, or some combination thereof. I believe that most Americans realize that the Intelligence Community exists to collect the vital intelligence that helps protect our nation from foreign threats. We focus on uncovering the secret plans and intentions of our foreign adversaries. But what we do not do is spy unlawfully on Americans, or for that matter spy indiscriminately on the citizens of any country. We only “spy” for valid foreign intelligence purposes as authorized by law with multiple layers of oversight to ensure we do not abuse our authority.”

Welcome to the Defense Security Service (DSS) Intelligence Oversight Awareness online training course.

All DSS employees—both Counterintelligence (CI) and non-counterintelligence, government or contractor—are required* to complete Intelligence Oversight training within 30 calendar days of their entry on duty and annually thereafter. This course has been developed to meet those requirements.

This course has two versions. “Version 1: CI” is intended for those DSS employees who have an intelligence mission (primarily in the Counterintelligence (CI) Directorate). “Version 2: non-CI” is intended for the remaining DSS employees who do not have an intelligence mission.

Click on the appropriate button to begin the course.

*(Defense Security Service Regulation Number 18-9, Intelligence Oversight Program, dated September 3, 2010)

DSS Mission

The Defense Security Service, or DSS, mission is to support national security and the warfighter, secure the nation's technological base, and oversee the protection of United States and foreign classified information in the hands of industry.

In support of this mission within DSS, there are multiple groups each with their own special charter. One of these groups is the DSS Counterintelligence (CI) Directorate, an intelligence component embedded within DSS whose mission is to identify unlawful penetrators of cleared U.S. defense industry and articulate the threat for industry and U.S. government leaders.
Defense Security Service
Intelligence Oversight Awareness
Training Course

Transcript for Non-CI

In order to accomplish this mission, it is imperative that all DSS personnel are aware of the Intelligence Oversight (IO) policy that governs the procedures involved in the collection, retention, and dissemination of information concerning United States persons.

Course Purpose

The purpose of this training is to ensure that those involved at any point in activities involving information about U.S. persons are aware of the following:

1) Under the mission and authority of DoD Manual 5240.01, there are specific restrictions placed on DoD intelligence components with regard to collecting and retaining U.S. persons information.

2) There are differences in how the DoD intelligence components can collect U.S. persons information and how someone acting in an industrial security or personnel security capacity under the mission and authority of the NISPOM can collect U.S. persons information.

The information in this course also includes guidance for those who discover activities of a questionable nature and how to recognize and report those activities to the proper authorities.

Course Objectives

By the end of this course, all DSS employees should be able to:

- Define Intelligence Oversight
- Explain the purpose of Intelligence Oversight
- Describe who or what is included in the term “U.S. Person”
- Define Intelligence Activity
- Recognize prohibited activities
- Know how to report questionable activities

EO 12333

Though not everyone within DSS is directly involved with intelligence information, everyone is responsible to report questionable activities as defined in this course and to treat any intelligence information according to regulations set forth in Executive Order (EO) 12333 and DoD Manual 5240.01 that protect intelligence information regarding U.S. persons.

It is important to note that personnel outside of CI cannot be tasked with or conduct intelligence activities.
Defense Security Service
Intelligence Oversight Awareness
Training Course
Transcript for Non-CI

What is Intelligence Oversight?

Intelligence Oversight (IO) is the process of ensuring that all DoD intelligence, counterintelligence, and intelligence-related activities are conducted in accordance with applicable U.S. law, Presidential Executive Orders, and DoD directives and regulations.

The DoD Intelligence Oversight program is designed to ensure that DoD can conduct its foreign intelligence and counterintelligence missions while protecting the statutory and constitutional rights of U.S. persons. It also provides for the reporting of questionable activities.

If someone other than an intelligence professional is acting in that capacity, whether they take it upon themselves or are given a task by someone who cannot perform the requested task, they will fall under the purview of DoD Manual 5240.01 as it pertains to U.S. person information.

For example, an Industrial Security Rep is allowed to retain a copy of a suspicious contact report that they have received from industry even if it contains U.S. person data because they are functioning in a security capacity and not as an intelligence professional.

DSS CI Collection Activities

The National Industrial Security Program Operating Manual, or NISPOM, requires cleared industry to report suspicious activities to the FBI and DSS. Those suspicious contact reports (SCRs) are passed from industry through the industrial security representatives to the counterintelligence office. Once in the possession of the counterintelligence office, the information contained within the SCR falls within the applicability of Intelligence Oversight requirements. In some cases, personnel security adjudicators come across questionable information contained in a personnel security investigation file that may be of counterintelligence concern. When that information is received by the DSS CI Office for further review and analysis, it too falls within the Intelligence Oversight guidelines.

Why do we need IO?

During the 1960s and early 1970s, the strong and often violent opposition to the Vietnam War and Civil Rights issues prompted many leaders at the highest levels of government to view groups involved in these issues not just as political threats but also as threats to civil order. In the belief that foreign governments were involved, military intelligence units and other government agencies were ordered to aggressively collect information about U.S. citizens engaged in the anti-war and Civil Rights Movements. Reaction to such "Big Brother" activities led to public demands for restraints on the intelligence community to protect against abuse of the Constitutional provision against unlawful search and seizure.
In 1976, Executive Order 11905 established the first rules on the collection, retention, and dissemination of information on U.S. persons. This process culminated in Executive Order 12333, which President Ronald Reagan signed in December 1981. Each president since President Reagan has endorsed this same executive order. This order was recently amended but remains essentially unchanged.

Although the abuse that brought about the Intelligence Oversight system occurred more than 30 years ago, Intelligence Oversight requirements remain current and relevant today, especially in light of the ongoing global war on terror and ever increasing threats by industrial espionage. By the nature of their jobs, DoD personnel are in contact with U.S. person information and therefore need to be aware of the need for increased Intelligence Oversight vigilance.

What is a U.S. Person?

“U.S. person” determination factors:

- United States citizens
- An alien known by the Defense Intelligence Component (DIC) to be a permanent resident alien
- Unincorporated associations substantially composed of U.S. citizens or permanent resident aliens
- A corporation incorporated in the U.S., except for a corporation directed and controlled by a foreign government or governments
- A corporation or corporate subsidiary incorporated abroad—even if partially or wholly owned by a corporation incorporated in the U.S.—is not a U.S. person
- A person or organization in the U.S. is presumed to be a U.S. person, unless specific information to the contrary is obtained: conversely, a person or organization outside the U.S. or whose location is not known to be in the U.S. is presumed to be a non-U.S. person, unless specific information to the contrary is obtained

Where can I get information on Intelligence Oversight Regulations?

Intelligence Oversight as authorized in Executive Order 12333 is implemented through DoD Manual 5240.01, entitled “Procedures Governing the Activities of DoD Intelligence Activities.” There are 10 procedures outlining the proper collection, retention, and dissemination of intelligence information on U.S. persons by the DoD intelligence components.

The focus of this training will include the following procedures of DoD Manual 5240.01:

- Procedure 1 deals with general provisions.
- Procedures 2 through 4 cover collection, retention, and dissemination of information
Defense Security Service
Intelligence Oversight Awareness
Training Course
Transcript for Non-CI

about U.S. persons.
- Procedure 10 deals with undisclosed participation (UDP) in organizations and exclusions contained within this manual.

The DoD Regulation 5240.1-R is still in effect for Procedures 11 through 15. This training will include:

- Procedure 14, which contains the employee responsibilities for conduct and required training.
- Procedure 15, which encompasses identifying, investigating, and reporting questionable intelligence activities.

Procedures 5-9 will not be addressed in this training since, under normal circumstances, DSS does not have the mission or authority to conduct the methodologies identified in those procedures.

Procedure 1: General Provisions

DoD intelligence components must not infringe upon the Constitutional rights of any United States person. Intelligence components must protect the privacy rights of all persons entitled to such protection. Their actions must be based on a lawfully assigned function and employ the least intrusive, lawful techniques. All actions must comply with regulatory requirements.

Important: This regulation does not in itself authorize intelligence activity. The DoD element must first have the mission and authority to conduct the intelligence activity. DoD Manual 5240.01 does not apply to law enforcement activities, including civil disturbance operations.

It is also important to note that DoD Manual 5240.01 does not apply to industrial security or personnel security activities. Those activities are defined in the National Industrial Security Program Operating Manual (NISPOM).

Procedure 2: Collection of Information

Collection is defined as: information collected when it is received by a Defense Intelligence Component (DIC), whether or not it is retained by the Component for intelligence or other purposes. Collected information includes information obtained by any means, including information that is volunteered to the Component.

Information that identifies U.S. persons can be collected if the information is necessary to perform a function assigned to DSS and the information fits into one or more of the defined categories of information types as defined in the next slide.

When authorized, intelligence components may collect U.S. person information by any lawful means, but they must exhaust the least intrusive collection means before requesting a more intrusive
Defense Security Service
Intelligence Oversight Awareness
Training Course
Transcript for Non-CI

method. To the feasible extent, information shall be collected from publically available information or with the consent of the person concerned.

Absolutely nothing in Procedure 2 can be interpreted as authority to collect information relating to a U.S. person solely because of that person’s lawful advocacy of measures opposed to Government policy.

DSS Counterintelligence (CI) is most likely to collect U.S. person information under category 4 and 6 as listed below. If it is a part of an assigned mission, then collection of this information is allowed. Retention of U.S. person material is subject to the strictures in DoD Manual 5240.01.

The following exemption categories are further defined in the handout available under the resources tab:

1. Publically Available Information, such as internet, news reports, and public records
2. Information Obtained with Consent (HR, IS Reps in an SSP)
3. Foreign Intelligence
4. Counterintelligence
5. Threats to Safety
6. Protection of Intelligence Sources, Methods, and Activities
7. Current, Former, or Potential Sources of Assistance to Intelligence Activities
8. Persons in Contact with Sources or Potential Sources
9. Personnel Security
10. Physical Security
11. Communications Security Investigation
12. Overhead and Airborne Reconnaissance
13. Administrative Purposes

Procedure 3: Retention of Information

Information is defined as retained only if it can be retrieved by the person’s name or other personal identifying data.

DSS can retain information concerning U.S. persons if it was collected pursuant to Procedure 2* and if the information fits into one or more of the following categories:

- Information could have been collected intentionally under Procedure 2. (This means it was a part of an assigned task or job responsibility.)
- Information is necessary to understand or assess foreign intelligence or counterintelligence.
- Information is foreign intelligence or counterintelligence collected from electronic surveillance.
- Information may indicate involvement in activities that violate Federal, state, local, or
Defense Security Service
Intelligence Oversight Awareness
Training Course
Transcript for Non-CI

foreign law.

DSS can retain U.S. person information not related to our mission or functions only long enough to refer to other agencies or to report Intelligence Oversight violations.

Access to U.S. person information will be restricted to certain individuals on a need-to-know basis. Intelligence components will conduct a quarterly review of their intelligence files, regardless of the type of record or where it is located or stored. This review will specifically focus on U.S. person information to determine whether continued retention serves the purpose for which it was retained and that continued retention is necessary to an assigned function.

An example of when U.S. person information might be collected legally but not retained would be if the intelligence professionals determine that the suspicious person reported by the IS Rep is not acting on behalf of a foreign power but is instead stealing proprietary information and conducting corporate espionage for a rival company. That activity, although illegal, would not be retained in a DSS intelligence database. All U.S. person data would be redacted and the case would be referred to the appropriate government agency that has the investigative authority for that crime.

*Information gathered by DSS employees in the course of their official duties.

**Procedure 4: Dissemination of Information**

This procedure governs the type of U.S. person information that may be disseminated without the person’s consent outside of the DoD intelligence component which collected and retained the information.

The DoD intelligence component may disseminate information concerning U.S. persons if it was collected, retained, or both, under Procedures 2* and 3**, and the recipient is reasonably believed to have a need to receive such information for the performance of a lawful governmental function and is one of the following:

- A DoD employee or contractor who has a need for such information in the course of his or her official duties.
- A law enforcement entity of federal, state, or local government and the information may indicate involvement in activities that may violate laws the recipient is responsible to enforce.
- An agency within the intelligence community.
- A federal government agency authorized to receive such information in the performance of a lawful government function.
- A foreign government when dissemination is undertaken pursuant to an agreement or other understanding with such government.

Any exceptions to dissemination must be approved by legal.
Procedure 10: Undisclosed Participation (UDP) in Organizations

Procedure 10 governs the participation of a Defense Intelligence Component (DIC) and anyone—including sources—acting on behalf of a DIC in any organization in the U.S. or any organization outside the U.S. that constitutes a U.S. person. The term “organization” includes corporations, other commercial entities, and associations formed for a social, political, fraternal, professional, business, academic, ethnic-affinity, or religious purpose, including those that meet and communicate through the use of technologies.

Anyone acting on behalf of a DIC may join, become a member of, or otherwise participate in an organization in the U.S.—or in any organization outside the U.S. that constitutes a U.S. person—if his or her intelligence affiliation is disclosed to an appropriate official of the organization. Without such disclosure, the other provisions of Procedure 10 must be applied to authorize a UDP.

Exclusions:

- Personal Participation: Activities conducted within an organization solely for personal purposes (i.e., activities undertaken upon the initiative and at the expense of a person for personal benefit)
- Voluntarily Provided Information: Activities conducted within an organization by any person who is already a member of the organization, or who joins on his or her own behalf, and later volunteers information to a DIC not in response to a specific request or DIC tasking.
- Publically Available Information on the Internet (e.g. Google Search): Collection of publically 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.

Procedure 14: Employee Conduct

Procedure 14 sets forth the responsibilities of employees of DoD intelligence components to conduct themselves in accordance with this Regulation and other applicable policy. It also provides that DoD intelligence components shall ensure, as appropriate, that these policies and guidelines are made known to their employees. Specifically, all DSS employees are required to receive an Intelligence Oversight briefing within 30 calendar days of initial assignment and annually thereafter.
Procedure 15: Questionable Intelligence Activities

This procedure provides for the identification, investigation, and reporting of questionable activities. DoD Components shall report the following matters to the Senior Intelligence Oversight Official (SIOO) in accordance with the Director of National Intelligence and Chairman, Intelligence Oversight Board Memorandum, “Intelligence Oversight Reporting Criteria,” and DoD 5240.1-R.

A Questionable Intelligence Activity refers to any conduct that constitutes, or is related to an intelligence activity that may violate the law, any Executive Order, or Presidential Directive, including E.O. 12333 (reference (a)) or applicable DoD policy including DoD Manual 5240.01. More information on Questionable Intelligence Activities can be found in the handout available under the resources tab.

Any development or circumstance involving an intelligence activity or intelligence personnel that could impugn the reputation or integrity of the DoD Intelligence Community or otherwise call into question the propriety of an intelligence activity is considered to be a Significant or Highly Sensitive Matter.

Be sure and review the Questionable Intelligence Activities Quick Reference Guide under the resource tab for detailed information on reporting procedures.

Examples of a Significant or Highly Sensitive Matter Activity

Significant or Highly Sensitive Matters might be manifested in, or by, an activity that falls into one of the following categories:

- It involves congressional inquiries or investigations.
- The matter may impact foreign relations or foreign partners.
- It is related to the unauthorized disclosure of classified or protected information, such as information identifying a sensitive source and method.

An example of this would be if a leak of the magnitude of “Wiki-leaks” occurred, but this time the leak occurred at a cleared defense contractor by a disgruntled employee that perhaps had access to multiple classified programs.

Reporting under this paragraph does not include reporting of routine security violations. Spillage occurring when classified information is inadvertently sent over an unclassified system would not normally be considered significant or a highly sensitive matter activity. This would be handled through an administrative inquiry.
Examples of Prohibited Activities

Here are several examples of intelligence activities that are prohibited under DoD Manual 5240.01.

A DSS intelligence professional cannot:

- Gather information on domestic groups within the U.S. that are not connected with a foreign power or international terrorism.
- Produce and disseminate intelligence threat assessments containing U.S. person information without a clear explanation of the intelligence purpose for which the information was collected.
- Collect U.S. person information from open sources without a mission or authorization to do so.

As a non-intelligence professional, you also cannot perform a questionable activity even if requested to do so by someone within CI.

Reporting Violations of IO Regulations

The following applies to all individuals in the DSS community:

- You are required to report questionable intelligence activities to the responsible authorities immediately.
- You may report through your chain of command starting with your supervisor, or if you feel your organization is pressuring you to do something questionable, you can also report it to the DSS Office of the Inspector General or DSS General Counsel.
- No reprisal or adverse action may be taken against personnel for reporting possible Intelligence Oversight violations.
- Conversely, adverse action may be taken against personnel who were aware of violations but failed to report them.

Summary

The purpose of Intelligence Oversight is to enable DoD components performing authorized intelligence functions to carry out those functions in a manner that protects the constitutional rights of U.S. persons. DoD Manual 5240.01 established the rules and procedures for collecting data on U.S. persons. Remember that the term "U.S. persons" includes U.S. citizens but is actually much broader.
The DSS *can* collect information that identifies a U.S person if the information is necessary to perform an Industrial Security function under the authority of the NISPOM or other authorized function.

All employees of DSS not only have the responsibility to report violations of Intelligence Oversight regulations, they must also report any questionable activities.

No reprisal or adverse action may be taken against personnel for reporting possible Intelligence Oversight violations.