# *Intelligence Oversight Awareness – Counterintelligence (CI) Track*

## Student Guide

February 2024

*Defense Counterintelligence and Security Agency*

## *Welcome*

Welcome to the DCSA Intelligence Oversight Awareness course.

In a 2013 testimony to Congress on Foreign Intelligence Surveillance, former Director of National Intelligence, retired Lieutenant General (LT GEN) James Clapper spoke about limitations to intelligence activities as pertaining to U.S. Persons.

LT GEN James Clapper (Retired) stated, “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 our activities have been characterized has often been incomplete, inaccurate, or misleading, or some combination thereof. I believe that most Americans realize 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 authorities."

## *Introduction*

All DCSA employees, both government and contractors, both Counterintelligence (CI), and non-counterintelligence (Non-CI), are required by DCSA regulations 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 tracks. Track 1, CI, is intended for those DCSA employees who have an intelligence mission primarily in the Counterintelligence Directorate. Track 2, Non-CI, is intended for the remaining DCSA employees who do not have an intelligence mission.

## *DCSA Mission*

DCSA has a unique mission within the Department of Defense that includes supporting national security and the warfighter. For a full reading of the agency’s mission, please visit the course resources.

In support of this mission within DCSA there are multiple groups with their own special charter. One of these groups is the DCSA CI and Insider Threat Directorate, a Defense Intelligence Component embedded within DCSA, whose mission is to identify unlawful penetrators of cleared U.S. defense industry and articulate the threat for industry and U.S. government leaders.

In order to accomplish this mission, it is imperative all DCSA personnel are aware of the DOD policy that governs intelligence authorities and the procedures involved in the collection, retention, and dissemination of U.S. Persons’ information.

## *Course Purpose*

The purpose of this training is to ensure those involved at any point in intelligence activities are conducting those activities properly. The intended audience for this course is all personnel conducting, supervising, or providing technical oversight of intelligence activities. It also applies to those who are involved in any other way in intelligence activities as per DOD Manual 5240.01 where intelligence activities refer to all activities that Department of Defense intelligence components are authorized to take pursuant to Executive Order (E.O.) 12333.

## *Course Objectives*

By the end of this course, individuals involved in intelligence activities should be able to:

- Explain the purpose of Intelligence Oversight
- Describe who or what is included in the term U.S. Person
- Delineate collection, retention, and dissemination procedures for U.S. Persons' information
- Identify where to find the proper collection, retention, and dissemination rules for U.S. Persons' information
- Recognize examples of prohibited activities
- Know how to report questionable activities

## *E.O. 12333*

Though not everyone within DCSA is directly involved with intelligence activities, everyone is responsible to report questionable activities as defined in the course and to treat any intelligence information according to regulations set forth in E.O. 12333 and DOD Manual 5240.01, especially in the protection of U.S. Persons' information. It is important to note that personnel outside of CI cannot be tasked to conduct Counterintelligence activities.

## *What is Intelligence Oversight?*

Intelligence Oversight is the process of ensuring all DOD intelligence and counterintelligence activities are conducted in accordance with applicable US law, Presidential E.O.s, and DOD issuances. 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.

## *DSCA CI Collection Activities*

The 32 CFR Part 117, National Industrial Security Program Operating Manual (NISPOM), requires cleared industry to report suspicious activities to the FBI and DCSA in the form of a Suspicious Contact Report (SCR).

SCRs submitted to DCSA are directed to the DCSA CI and Insider Threat Directorate. And, once in the possession of the Counterintelligence Directorate, 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 which may be of counterintelligence concern. When that information is received by the DCSA CI Directorate for further review and analysis, it too falls within the Intelligence Oversight guidelines.

## *Why do we need Intelligence Oversight?*

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 anti-war and Civil Rights movements. Reaction to such "Big Brother" activities led to public demands for curbs on the intelligence community to protect against abuses 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.

Although the abuses that brought about the Intelligence Oversight system occurred many 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, DCSA personnel are in contact with U.S. Person information and therefore need to be aware of the need for increased Intelligence Oversight vigilance.

## *Determining a U.S. Person*

U.S. Person determination factors are as follows:

- A U.S. citizen.
- An alien known by the Defense Intelligence Component to be a permanent resident alien.
- An unincorporated association substantially composed of U.S. citizens or permanent resident aliens.
- A corporation incorporated in the United States, 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 United States, is not a U.S. Person.
- A person or organization in the United States is presumed to be a U.S. Person, unless specific information to the contrary is obtained.
- Conversely, a person or organization outside the United States, or whose location is not known to be in the United States, 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?*

Intelligence Oversight, as authorized in Executive Order 12333, is implemented through DOD Directive 5148.13 entitled "Intelligence Oversight." DOD Manual 5240.01 entitled "Procedures Governing the Conduct of DOD Intelligence Activities" outlines the procedures for proper collection and dissemination of U.S. Person information by DOD 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 U.S. Persons' information.
- Procedures 5 through 10 will not be addressed in this training since, under normal circumstances DCSA has very limited or no authority to conduct the methodologies identified in those procedures.

This training will include the employee responsibilities for conduct and required training and encompasses identifying, investigating, and reporting questionable intelligence activities.

## *Procedure 1: General Provisions*

DOD Intelligence Components must not infringe upon the Constitutional rights of any U.S. 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 all regulatory requirements.

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

Procedure 1 includes guidance on the access and use of U.S. Persons' Information obtained from shared repositories.

## *Procedure 2: Collection of U.S. Persons' Information (USPI)*

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

U.S. Persons' Information (USPI) can be collected if necessary to perform a function assigned to DCSA and the information fits into one or more of the defined categories of information types below.

When authorized, Intelligence Components may collect USPI by any lawful means, but they must exhaust the least intrusive collection means before requesting a more intrusive method. To the extent feasible, information shall be collected from publicly 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.

The following exemption categories are further defined in the handout available on the course resources page.

1. Publicly Available Information
2. Consent
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.

You may not file unauthorized USPI just because it is not retrievable by reference to a person's name or other identifying data - that would not be within the spirit and intent of E.O. 12333. Finished intelligence products in a database are considered retained because they can be searched by a person's name or other identifiable information like a Social Security Number (SSN), a driver's license number, or an automobile license plate number.

DCSA can retain USPI if it was collected pursuant to Procedure 2, and it's information gathered by DCSA employees in the course of their official duties, and if the information:

- Could have been collected intentionally under Procedure 2. This means it was a part of an assigned task or job responsibility.
- Or is necessary to understand or assess foreign intelligence or counterintelligence.

DCSA can retain USPI not related to our mission or functions only long enough to refer to other agencies or to report Intelligence Oversight violations.

DCSA CI personnel will evaluate the information promptly to determine if intelligence information may be permanently retained. If necessary, the Component may retain the information for evaluation for up to five years.

Procedure 3 stipulates Components will use reasonable measures to identify, mark, or tag files reasonably believed or known to contain USPI, regardless of the format or location of the information or method of storing it. Components will also individually mark files and documents containing USPI.

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

## *Procedure 4: Dissemination of Information*

This procedure governs the types of USPI 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 USPI 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.

An example of information that could be collected, retained, and disseminated would be the suspicious activity reported to DCSA that is both of counterintelligence value AND determined to be acting on behalf of a foreign power. That information, even if it is a U.S. Person, could be retained in a DCSA intelligence database and disseminated to the governmental agency that has the proper investigative authority. In this particular case, that authority would be either a military department counterintelligence investigative agency or the FBI, or both.

Any exceptions to dissemination requires review.

## *Questionable Intelligence Activities*

Directive 5148.13 provides for the identification, investigation, and reporting of questionable intelligence activities (QIAs) and significant or highly sensitive matters (SHSMs). A QIA refers to any intelligence or intelligence related activity when there is a reason to believe such activity may violate the law, any Executive Order or Presidential Directive, including Executive Order 12333, or applicable DOD policy. More information on QIAs can be found in the handout available on the course resources page.

Be sure and review the Questionable Intelligence Activities Quick Reference Guide on the course resources page for detailed information on reporting procedures. An SHSM refers to 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.

## *Examples of a Significant or Highly Sensitive Matter Activity*

SHSMs might be manifested in, or by, an activity that falls into one of the following categories in that the matter:

- Involves congressional inquiries or investigations.
- May result in adverse media coverage.
- May have impact on foreign relations or foreign partners, or
- Is related to the unauthorized disclosure of classified or protected information, such as information identifying a sensitive source and method.

Reporting under this procedure does not include reporting of routine security violations.

## *Prohibited Activities*

Here are several examples of intelligence activities that are prohibited under DOD Manual 5240.01:

- Gathering information on domestic groups within the United States that are not connected with a foreign power or international terrorism.
- Producing and disseminating intelligence threat assessments containing USPI without a clear explanation of the intelligence purpose for which the information was collected.
- Collecting U.S. Person information from open sources without a mission or authorization to do so.
- Using intelligence access and tools to conduct research on spouse, child, or other persons for personal gain.
- Using your access, intelligence position, or intelligence credentials for other than official business.

## *Reporting Violations of Intelligence Regulations*

The following applies to all individuals in the DCSA community:

- You are required to report QIAs and SHSMs immediately UPON DISCOVERY through your chain of command or supervisor to the DCSA Intelligence Oversight and Compliance Office (IOCO)
- You can also report QIAs or SHSMs to the DCSA General Counsel (GC), or to the DCSA Inspector General (IG), or to the DOD GC, or to the DOD SIOO, or to the Joint Staff IG, or the Legal Counsel for Chairman Joint Chiefs of Staff (CJCS), or to the DOD IG, or to the Intelligence Community IG.
- No reprisal or adverse action may be taken against personnel for reporting possible 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 the term U.S. Persons includes U.S. citizens but is actually much broader.

DCSA can collect U.S. Persons' information if necessary to perform an Industrial Security function under the authority of the NISP or other authorized function assigned to DCSA and the information fits into one of the 13 information categories.

DCSA personnel have the responsibility to report questionable activities. No reprisal or adverse action may be taken against personnel for reporting possible Intelligence violations.