



# NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

## *Instructor-Led Training Course Descriptions*

### **ICD 704 PERSONNEL SECURITY COURSE**

**PURPOSE:** This course prepares you to make adjudicative decisions consistent with ICD 704 requirements. We will present approaches to enhance best practices and reciprocity across the Intelligence Community and Department of Defense organizations authorized to grant access and adjudicate for Sensitive Compartmented Information. This is an excellent seminar for security professionals who want to better understand the process behind adjudication decisions.

**LENGTH:** 2.5 days / A Option: Monday-Tuesday 8:00a-4:30p, Wednesday 8:00a-11:30a

B Option: Wednesday 1:00p-4:30p, Thursday-Friday 8:00a-4:30p

**PREREQ:** The enrollment process cannot be completed until you provide the certificates of completion for the following prerequisite courses.

1. The 13 Adjudicative Guidelines
2. Introduction to DoD Personnel Security
3. Introductions to National Security Adjudications

These prerequisites can be found at <http://www.cdse.edu/catalog/personnel-security.html>. Send certificates of completion to [NCSC-Training@dni.gov](mailto:NCSC-Training@dni.gov).

### **ICD 705 PHYSICAL SECURITY COURSE**

**PURPOSE:** The ICD 705 Physical Security Course: Lifecycle of A SCIF will prepare you to implement the requirements of the new ICD 705 series documents (ICD 705; ICS 705-1; ICS 705-2 and the ICD 705 Technical Specifications). The course is designed using a SCIF lifecycle theme:

- Phase I: Threat Definition and Planning
- Phase II: Preliminary Construction Planning
- Phase III: Design and Construction Requirements
- Phase IV: Accreditation
- Phase V: SCIF Operations and Management
- Phase VI: Disposal of a SCIF

The course stresses comprehension and construction best practices and application of the ICD 705 series documents.

**LENGTH:** 2.5 days / Monday-Tuesday 8:00a-4:30p, Wednesday 8:00a-11:30a OR Wednesday 1:00p-4:30p, Thursday-Friday 8:00a-4:30p

**PREREQ:** The enrollment process cannot be completed until you provide the certificates of completion for the following prerequisite courses.

1. The SCIF Physical Security Virtual

These prerequisites can be found at <http://www.cdse.edu/catalog/physical-security.html>. Send certificates of completion to [NCSC-Training@dni.gov](mailto:NCSC-Training@dni.gov).

## **SPECIAL SECURITY OFFICER COURSE (SSOC)**

**PURPOSE:** Prepare security professionals who administer SCI programs. We use practical implementation exercises to give hands-on experience. The topics include:

- Structure of Intelligence Community
- Security Incidents and Investigations
- Business and Security Interfaces
- Security Awareness, Training, and Education Programs
- Physical Security (ICD 705)
- Personnel Security (ICD 704)
- Information Systems Security (ICD 503)

**LENGTH:** 2.5 days / Monday-Tuesday 8:00a-4:30p, Wednesday 8:00a-11:30a OR Wednesday 1:00p-4:30p, Thursday-Friday 8:00a-4:30p

**PREREQ:** The enrollment process cannot be completed until you provide the certificates of completion for the following prerequisite courses.

1. Security Policies, Principles and Programs GS140.06
2. Introduction to Personnel Security PS113.06
3. Introduction to Physical Security PY011.06

These prerequisites can be found at <http://www.cdse.edu/catalog/index.html>. Send certificates of completion to NCSC-Training@dni.gov.

## **INSIDER THREAT HUB OPERATIONS COURSE**

**PURPOSE:** This is a new course to introduce and exercise the basic functions of an Insider Threat program's centrally managed analysis and response capability (referred hereinafter as the "Hub") to gather, integrate, analyze, and respond to potential insider threat information derived from counterintelligence, security, information assurance, human resources, law enforcement, and other internal and external sources. This is a practical, scenario-based course designed to expose Insider Threat personnel to realistic events in the day-to-day operations of an Insider Threat Hub. The class will include break out teams with an assigned instructor/facilitator for specialized attention. This course supersedes the previous National Insider Threat Task Force's (NITTF's) "Establishing and Operating an Insider Threat Program", "Principles of Hub Operations: Insider Threat Course", and "Principles of Hub Operations Course". The topics include:

- Insider Threat Program Hub Functions
- Legal Considerations
- Classification of Insider Threat information
- Inquiry fundamentals
- Response actions and Referrals
- Reporting and Documentation concepts

**LENGTH:** 3 days / 8:00 – 4:30

**PREREQ:** Insider Threat Program Manager/Senior Official must send e-mail concurrence to NCSC-Training@dni.gov for participant(s) enrollment at time of registration. Prerequisite training includes CI & Security Awareness Training, and Insider Threat Awareness Training. Prefer participants hold certificates in at least one of previous Insider Threat courses and be familiar with the Insider Threat Security Classification Guide.

OBJECTIVES:

- Understand the functions of Insider Threat Hub Operations
- Describe the policies and processes for Hub functions to effectively gather information
- Understand the legal considerations in establishing information flow processes, and handling information from a variety of internal and external sources
- Demonstrate how to gather and document counterintelligence, security, information assurance, human resource, law enforcement, and other information related to potential Insider Threat activities.
- Demonstrate how to integrate and analyze relevant information on potential Insider Threat activities.
- Demonstrate how to complete plans and reports with recommendations for follow-on actions in response to potential Insider Threat activities.
- Practical Exercises to Reinforce Learning