ODNI/NCIX
SPECIAL SECURITY CENTER
Security Education & Training Program
Course Descriptions

PLEASE READ:

- *Contractors must have approving Government Supervisor, POC or COTR email* **dni-ssc-training@dni.gov** *with concurrence for attendance*
- *Clearance verified in Scattered Castles/JPAS; do not send unless requested*
- *No costs to you or sponsoring agency for course participation. You are responsible for your travel/hotel/perdiem*
- *Courses may have students from our Commonwealth Partner Countries. Please contact us if this may impact your attendance.*

DNI/SSC ICD 503 - IT SYSTEMS SECURITY RISK MANAGEMENT, ASSESSMENT & AUTHORIZATION FOR THE INTELLIGENCE COMMUNITY COURSE

PURPOSE: This course is designed for Information System Security and Information Assurance Professionals responsible for implementing and assessing security policies, practices, procedures and technologies. The course will cover implementation and conduct of Intelligence Community (IC) information systems assessment, authorization, risk management and continuous monitoring in accordance with ICD 503. We will provide students with new methods and approaches to assessing and authorizing IT systems within the Intelligence Community. The course will deliver applicable national security level guidelines and methodologies with specific focus on IC Standards, plans, methods, processes, and templates. You will become familiar with IC 503 templates and processes through case studies and exercises.

LENGTH: 5 days / 8:00 – 4:30 (8:00 – 12:30 on Friday)

TARGET: Federal government civilians, military personnel, State, Local and Tribal governments, Commonwealth Partners and government contractors who are directly involved in the assessment and authorization of IC information systems in accordance with ICD 503 and associated IC Standards. The subject matter expertise addressed in the seminar are (ICD 503):
- System Categorization
- Security Controls and Assessment
- Risk Assessment
- System Authorization
- Continuous Monitoring
- Protection of IT equipment and media

MATERIALS: This course is taught at the **UNCLASSIFIED** level.

PREREQ.:
- Knowledge of ICD 503, 'Information Technology Systems Security Risk Management, Certification, and Accreditation;
- Experience and/or knowledge of DCID 6/3, JFAN 6/3 or DIACAP;
- Understanding of IT networks, systems, terminology and System Development Life Cycle (SDLC)
- Familiarization with NIST Special Publication 800-37 Revision 1, 'Guide for Applying the Risk Management Framework to Federal Information Systems', CNSSI 1253, and NIST SP 800-53 Revision 3, SP 800-39, SP 800-30.

DNI/SSC ICD 704 ADJUDICATIONS COURSE

PURPOSE: This course prepares you to make adjudicative decisions consistent with ICD 704 requirements. We will provide approaches to enhance best practices and reciprocity across the Intelligence Community and DoD organizations authorized to grant access and adjudicate for Sensitive Compartmented Information. We will explain the adjudication process and what needs to be considered to upgrade an individual to another clearance and/or access level. Also an excellent seminar for a security professional who wants to understand the process behind adjudication decisions.

LENGTH: 5 days / 8:00 – 4:30 (8:00 – 12:30 on Friday)

TARGET: Personnel performing background checks, clearance upgrades and adjudications. Also to enhance knowledge for the well rounded career security professional.

MATERIALS: **UNCLASSIFIED w/classified discussions**

PREREQ.:

- **SECRET clearance**
- Please review ICD 704 prior to attending course.

DNI/SSC ICD 705 PHYSICAL SECURITY COURSE

PURPOSE: This course prepares you to implement the construction and security protection standards required for all US Government facilities or US Government sponsored contractor facilities where Sensitive Compartmented Information (SCI) or Special Access Program (SAP) material may be stored, used, discussed and/or processed. Discussion includes planning and defining requirements, site selection, design, construction, certification and accreditation, operations, and disposal. You will discuss current physical security concerns of their respective organizations and brainstorm solutions.

LENGTH: 5 days / 8:00 – 4:30 (8:00 – 12:30 on Friday)

TARGET: Federal government civilians, military personnel and government contractors responsible for the physical planning and implementation of SCI and SAP facilities.

MATERIALS: **UNCLASSIFIED w/classified discussions**

PREREQ.:

- **SECRET clearance**
- Please review the following documents prior to course attendance:
    - IC Directive 705, Sensitive Compartmented Information Facilities (SCIFs)
    - IC Standard 705-1, Physical and Technical Standards for SCIFs
    - IC Standard 705-2, Standards for Accreditation and Reciprocal Use of SCIFs

DNI/SSC SPECIAL SECURITY OFFICER COURSE (SSOC)

PURPOSE: Prepare security professionals who administer SCI programs. We will familiarize you with security DCIDs and SCI policies and compartments. We use practical implementation exercises to give hands-on experience. The class is divided into teams with an assigned facilitator for individual attention.   The topics include:
- Structure of Intelligence Community
- Security Incidents and Investigations
- Business and Security Interfaces
- Special Access Programs
- Physical Security (ICD 705)
- Personnel Security (ICD 704)
- Information Systems Security (ICD 503) experience

LENGTH: 5 days / 8:00 – 4:30 (8:00 – 12:30 on Friday)

TARGET: Security professionals who administer all aspects of SCI programs

MATERIALS: **UNCLASSIFIED w/classified discussions**

PREREQ.:

- Attendees must have **TS/ SCI** and 2-5 years security experience

- **Government personnel ONLY**

DNI/SSC MID-LEVEL SECURITY PROFESSIONAL SEMINAR (MSPS)

PURPOSE: Expose mid-level security officers to security issues and perspectives that prepare them for positions of greater responsibility in the security profession. The MSPS is the middle step in a three level comprehensive training development hierarchy for IC Security Professionals. The MSPS contains practical implementation exercises to give hands-on experience. The class is divided into teams with an assigned instructor/facilitator for individual attention. The topics include:
- Security Challenges Ahead
- Security from Multiple Perspectives
- IC Security Policy: Changes and Current Trends
- Analytical Risk Management (Mid-Level)
- Supervisory Growth and Management Challenges
- Leading an Effective Security Organization
- Information Systems Security in Transition
- Physical and Technical Security in Transition
- Personnel Security Today
- Achieving Excellence in Security Management
- Being a Security Leader of Integrity
- Communicating Security for Success
- Decision Making for the Security Manager
- Making the Most of Your Security Career

LENGTH: 5 days / 8:00 – 4:30 (8:00 – 12:30 on Friday)
TARGET: Security Managers who administer all aspects of SCI programs
MATERIALS: **UNCLASSIFIED w/classified discussions**
PREREQ.:
- Attendees must have **TS/ SCI** and 5-10 years security experience/GS11-GS13
- **Government personnel ONLY**

DNI/SSC SENIOR SECURITY PROFESSIONAL SEMINAR (SSPS)

PURPOSE: Expose the "next generation" of security managers and leaders to community best practices and provide a resource for developing effective program managers and leaders. Best practices and management philosophies will be woven throughout the seminar. We will engage participants in highly interactive discussions with top-notch security practitioners as presenters and facilitators. Exercises are utilized throughout the week to emphasize learning points and facilitate discussions. Each day will have a primary focus discussing principles in managing complex and integrated security programs. The topics include:

- Conflict Resolution
- Motivation by Communication
- Decision Making
- Advanced ARM
- Violence in the Workplace
- Security Management in a New Decade
- Foundations of a CI Profession
- Security Hot Topics
- Spotlight Panel (security leaders from different IC agencies)
- Keynote guest speakers from different IC agencies

LENGTH: 5 days: begins on Sunday at 4pm and concludes Friday noon (must stay on-site)

TARGET: Security professionals and managers

COST: You are responsible for per diem for accommodations and meals

MATERIALS: **UNCLASSIFIED**

PREREQ.: --Government Personnel Only GS 14-15 or equivalent with minimum 10 years security experience

Requires an emailed letter of recommendation from organizational supervisor to
dni-ssc-training@dni.gov

DNI/SSC SENSITIVE COMPARTMENTED INFORMATION (SCI) OVERVIEW SEMINAR

The courses below are currently being converted into Web-based training. Consideration will be made to hold a course live on-site by request, with a minimum of 75 participants. Contact dni-ssc-training@dni.gov for more information.

PURPOSE: **Module 1- Welcome to Intelligence Community (IC) Security:** A thorough SCI security exposure for recently SCI-approved personnel, or for those that do not handle SCI as part of their daily work lives. The session allows you to walk away with a solid security foundation and an understanding of your responsibilities. It provides basic knowledge needed to protect classified activities, procedures, systems, and facilities.

Module 2 – Intelligence Community Security Today: Highlight key security points from Module 1, and provide a greater focus on changes within security in a post 9/11 world. This session is useful as a refresher for security practitioners, and as an update of current security changes.

Module 3 - Classification Management: Provide a general understanding of classification management and how to properly mark documents. This session explains the basic elements of classification management, what we are protecting and how to do it. You will be briefed on safeguarding procedures, the basic elements of E.O. 12958, derivative classification authorities and we conclude with a classification exercise.

Module 4 – Unauthorized Disclosures: Explains problems surrounding unauthorized disclosures and provides security officers the tools to effectively respond to issue of unauthorized disclosures. You will be briefed on the laws and will gain insight into damage done by unauthorized disclosures. We will also explain responsibilities and requirements under ICD 701.

Module 5 – Living Within a Sensitive Compartmented Information Facility (SCIF): Expose attendees to principles and practices for the protection and management of information within the confines of a SCIF. A basic overview of access control, escorting visitors, how the SCIF is constructed, how to store information, and general policies that govern SCIFs and those that work in them. There will be an overview regarding SCI materials as well as classification management and how to ensure information stored within the SCIF is managed correctly. The course will include interactive discussions and exercises to emphasize learning points and facilitate discussions.

LENGTH: Modules 1,2,3,4 = 3 hours each. Module 5 = 7 hours. Modules are stand-alone. If selecting Modules 1-4, please select at least 2 modules.

TARGET: Federal government civilians, military personnel and government contractors with responsibility for briefing newly SCI-cleared personnel. Also may be used for newly SCI-accessed personnel or for an annual refresher briefing.

MATERIALS: **UNCLASSIFIED w/classified discussions**

PREREQ.: Attendees must have **TS** for #1,2,5.