

Organization Chart

Community Services Division

Oversight & Liaison Division

Policy & Planning Division

CAPCO Division

SSC Portal

Joint Suitability and Security Clearance Reform Team

ODNI

Welcome

The Director of National Intelligence (DNI) Special Security Center (SSC) is the Intelligence Community (IC) source for security policies, advice and guidance on security practices and procedures, security-relevant issues, and security tools. It is the Center for security expertise, analysis and the tools that the IC relies on to balance the need to protect with the need to appropriately share intelligence information.



Welcome to the DNI Special Security Center (SSC)

The SSC exists to assist the DNI, in his dual role as head of the Intelligence Community (IC), and as the Security Executive Agent for US Government security clearance programs (pursuant to Executive Order 13467). SSC assists in the execution of DNI responsibility to share and protect national intelligence information throughout the IC, the US government, US contractors, state and local officials and our foreign partners. The SSC's objectives include:

- Fostering IC security uniformity and reciprocity
- Performing policy review, coordination and formulation
- Promoting uniform application of security policy
- Assessing, advising and reporting to the DNI on the implementation of security policies
- Enabling the Community-wide exchange of critical security data
- Providing services of common concern in the areas of security research, training and database management

SSC Executes DNI responsibilities as Security Executive Agent to drive efforts to achieve government-wide improvements to clearance process timeliness and effectiveness, reciprocal recognition of security clearances and access approvals, and to modernize security business practices in the US Government. SSC hosts a joint program management activity ("Joint Team") to develop and implement reforms across the Executive Branch, to include the IC. Joint Team reform efforts are responsive to the direction of the Suitability and Security Clearance Performance Accountability Council, established pursuant to E.O. 13467.

This page is maintained by the DNI Special Security Center Office.







































1 of 1 7/18/2012 8:52 AM **ODNI**



This page is maintained by the DNI Special Security Center Office.









































7/18/2012 8:51 AM 1 of 1



Organization Chart

Community Services Division

Oversight & Liaison Division

Policy & Planning Division

CAPCO Division

SSC Portal

Joint Suitability and Security Clearance Reform Team

ODNI

Home :: Community Services Division (CSD) :: Security Databases Program

Scattered Castles

The Intelligence Community Security Clearance Repository, commonly known as Scattered Castles, is an up-to-date, authoritative source of clearance and access information on approximately 2 million IC and Department of Defense personnel. Scattered Castles is hosted as Community of Interest (COI) on the Joint Worldwide Intelligence Communication System (JWICS). The scope of the Scattered Castles Program is to provide a common, trusted repository of individuals' clearance and accesses, easily accessible by a controlled set of security professionals within the IC with a valid need to verify clearance and access information.

SCIF Repository

The SCIF Repository provides a single source of secure facilities information world-wide within the Intelligence Community. This repository provides the ability for a select group of security personnel with a valid need for information regarding accredited facilities to access data provided by IC agencies. It provides an invaluable tool to the DNI and senior IC managers in times of crisis in identifying sites in jeopardy due to natural disasters, heightened security alerts, and domestic and international hostilities. The repository provides accreditation information, co-use agreements in place, and other information such as location and contact information.

Information Portals

The Special Security Center has an U//FOUO Information Portal which operates on the Internet, and a TS//SCI Information Portal on JWICS. The portals provide standardization of security-related functions and valuable services to the Intelligence Community, Department of Defense, and the Non-Title 50 agencies. The portals also provide those individuals with security responsibilities in government and industry with a suite of tools and other features designed to enhance their work, to save both time and money, and to support the increased degree of Security Community-wide cooperation and collaboration.

This page is maintained by the DNI Special Security Center Office.





































1 of 1 7/18/2012 8:42 AM

DNI/NCIX



Community Education & Training Group **Security 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/per diem
- Courses may have students from our Commonwealth Partner Countries. Please contact us if this may impact your attendance.

DNI/NCIX 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.

4 days / 8:00 - 4:30 LENGTH:

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.

Revised 7-1-11 Page 1 of 5

DNI/NCIX 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/NCIX 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:
 - o IC Directive 705, Sensitive Compartmented Information Facilities (SCIFs)
 - IC Standard 705-1, Physical and Technical Standards for SCIFs
 - o IC Standard 705-2, Standards for Accreditation and Reciprocal Use of SCIFs

DNI/NCIX 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/NCIX 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

PREREO .:

- Attendees must have TS/ SCI and 5-10 years security experience/GS11-GS13
- Government personnel ONLY

DNI/NCIX 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:

- Launching Leadership in Security
- Conflict Resolution
- Building a Successful Security Program
- Workplace Violence Tools for Security
- Motivation by Communicating Security Message
- Decision Making for Today's Security Professional
- 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/NCIX 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.



ODNI/ONCIX

Security Education & Training Group Offerings for Aug 2011 - Jul 2012

	ICD 503 Information Security Course for Implementers & Assessors	ICD 704 Adjudications Course	ICD 705 Physical Security Course	Special Security Officer Course (SSOC) (GOV only)	Mid-Level Security Professional Seminar (MSPS) (GOV only)	Senior Security Professional Seminar (SSPS) (GOV only, by nomination)
AUG 2011	8-11> Chantilly, VA 15-18> Chantilly, VA **17-18 > DM&A Chantilly 22-26> Chantilly, VA	1-5> Chantilly, VA FULL	8-12> Chantilly, VA FULL		22-26> Chantilly, VA FULL	
SEP 2011	12-15> Chantilly, VA 19-22> Chantilly, VA 26-29> Chantilly, VA	12-16> Linthicum, MD FULL	12-16> Linthicum, MD FULL	26-30> Chantilly, VA FULL		25-30> Shepherdstown, WV
OCT 2011	10/31-11/3> Chantilly, VA	17-21> Chantilly, VA FULL	3-7> Chantilly, VA FULL			
NOV 2011	11/28-12/1> Chantilly, VA	10/31-11/4> Linthicum, MD FULL	10/31-11/4> Linthicum, MD FULL	14-18> Chantilly, VA FULL	14-18> Chantilly, VA FULL	
DEC 2011	12-15> Chantilly, VA		5-9> Chantilly, VA FULL	5-9> Chantilly, VA FULL		
JAN 2012	23 - 27> Chantilly, VA	9-13> Chantilly, VA	23-27> Linthicum, MD FULL			
FEB 2012	27- 3/2> Chantilly, VA		13-17> Chantilly, VA FULL	6-10> Chantilly, VA FULL		
MAR 2012	26-30> Chantilly, VA	12-16> Linthicum, MD	12-16> Linthicum, MD FULL		26-30> Chantilly, VA	
APR 2012	30 - 5/4> Chantilly, VA	9-13> Chantilly, VA	16-20> Chantilly, VA	2-6> Chantilly, VA		15-20> Harbourtowne, MD
MAY 2012	7-11> Chantilly, VA		7-11> Chantilly, VA		14-18> Chantilly, VA	
JUN 2012	18-22> Chantilly, VA	11-15> Linthicum, MD	11-15> Linthicum, MD	18-22> Chantilly, VA	25-29> Chantilly, VA	
JUL 2012	23-27> Chantilly, VA		9-13> Chantilly, VA			15-20> Harbourtowne, MD
	M - Th 8:00 - 4:30 Fri 8:00 - 12:30	M - Th 8:00 - 4:30 Fri 8:00 - 12:30	M - Th 8:00 - 4:30 Fri 8:00 - 12:30	M - Th 8:00 - 4:30 Fri 8:00 - 12:30	M - Th 8:00 - 4:30 Fri 8:00 - 12:30	Mandatory Overnight Stay at Facility

^{**}DM&A is a two -day course for Decision makers and Acquisition Staff

Cryptome

DNI/CIA Campus 13900 Air & Space Museum Parkway Chantilly, VA Property also known as Dulles Discovery North Google Earth Imagery, January 31, 2011





DNI/NCIX

Community Education and Training Group Course Request Form

REGISTRATION: *email this completed form to* <u>dni-ssc-training@dni.gov</u>. *State your name/* requested course/dates in the subject line of email. Courses may have students from Commonwealth Partner Countries. Please contact us if this may impact your attendance.

APPROVALS:

- Contractors requesting attendance must have Government Supervisor, POC or COTR email dni-ssc-training@dni.gov with concurrence for attendance when sending in form.
- SSPS requires an emailed letter of recommendation from organizational supervisor
- SSOC, MSPS and SSPS courses are for government personnel ONLY (see course description)
- We verify clearance information in Scattered Castles; do not send unless we request

COSTS: No costs to you or sponsoring agency for course participation, but you are responsible for travel/hotel/perdiem

Please fill in ALL fields Please fill in ALL fields

Course Requested: Click to SELECT From Pulldown Menu								
Date: 1 st choice: 2 nd choice: (see calendar)								
Your Legal Name:								
Gov. Organization: SEE NEXT DROP DOWN FOR MORE SELECTIONS responses of "Other" in comments box)								
Are you a Contractor? <i>(MUST check)</i> YES NO If yes, name of company:								
Geographic Location: SELECT ONE or a State> States A-M: N/A States N-W: N/A								
Job Title: (click box once and begin typing) Grade/Rank:								
E-mail (unclass): Phone (unclass) (ex: xxx-xxxx):								
Years Exp. in subject/class field: None Years you have held a clearance: None								
Date of Birth (ex: 4/22/1963) last 4 digits of SSN								
Government Supervisor EMAIL (unclass): (REQUIRED to register) Government Supervisor phone (unclass): (REQUIRED to register)								
Please indicate if you have any special needs: Additional Comments:								
We will condivous								

- We will send you:
 - 1. Confirmation of receipt of registration within 1 week
 - 2. Welcome packet with information/directions via e-mail approximately one month prior to course
 - 3. Reminder e-mail sent one week prior to the course

For any questions, contact: dni-ssc-training@dni.gov

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

SPECIAL SECURITY CENTER

Serving the Security Community

Welcome

home :: Community Services Division (CSD) :: Course Descriptions

Organization

Chart

Community Services

Division

Oversight & Liason Division

Policy & Planning Division

CAPCO Division

SSC Portal

Joint Suitability and Security Clearance Reform Team

ODNI

APPROVALS:

Contractors requesting attendance must have approving Government Supervisor, POC or COTR email dni-ssc-training@dni.gov with concurrence for attendance

We verify clearance information in Scattered Castles/JPAS; do not send unless we request

GSSOC, MSSOC and SSPS courses are for government personnel ONLY

COSTS

There are no costs to you or sponsoring agency for course participation

You are responsible for own travel/hotel/per diem

Course Descriptions

DNI SSC SCI Overview Seminar (Parts 1, 2 & 3)

PURPOSE:

- 1- Welcome to SCI: 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 be successful in the protection of classified activities, procedures, systems, and facilities. The session also provides an historical perspective as well as the impact of events on modern day security.
- **2- SCI Today:** Highlight key security points from Part 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.
- **3- Protection of Sources and Methods**: Explain problems surrounding unauthorized disclosures and provide 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.

LENGTH: 3 hours each. Held at your site by request. Choose 2 of the three above.

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/ SCI & have signed the NDA for parts 1 and 2. Part 3 is unclassified.

DNI SSC CLASSIFICATION MANAGEMENT BRIEF

PURPOSE:

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.

LENGTH: 3 hours. Held at your site by request.

TARGET: Federal government civilians, military personnel and government contractors that handle classified

documents.

MATERIALS: UNCLASSIFIED

PREREQ.: None.

DNI/SSC Life in A SCIF

PURPOSE: 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: 2 days / 8:00 - 4:30

TARGET:

Federal government civilians, military personnel and government contractors with access to an SCI facility (SCIF). Ideal for newly SCI-accessed personnel or those that do not handle SCI material on a regular basis.

MATERIALS: UNCLASSIFIED w/classified discussions

PREREQ.: Attendees must have TS/ SCI.

DNI/SSC DCID 6/3 Information System Security Basic Course

PURPOSE:

Designed to provide IS Security professionals with the knowledge, tools, understanding, and skill base to properly implement or oversee all security requirements in DCID 6/3. This training not only teaches the DCID 6/3 policy, procedures, and regulations, but allows to put into practice what the regulation requires. This is accomplished by participating in "real life" type exercises so that learned experiences may be taken back to the worksite. The security professional will leave with confidence to conduct any phase of the C&A process and have the skill base to keep compliant with DCID 6/3 throughout its Life Cycle. Covers Protection Level 1 and 2 only.

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

TARGET: Federal government civilians, military personnel and govt. contractors with responsibility for

overseeing or implementing DCID 6/3 security requirements.

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

PREREQ.: Knowledgeable of DCID 6/3, "Protecting Sensitive Compartmented Information within Information

Systems."

DNI/SSC ICD 704 Adjudicator Training Seminar (formerly DCID 6/4)

PURPOSE:

Prepare individuals 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 what goes into the adjudication process and what needs to be considered during a review to upgrade an employee to another clearance and/or access level. This is also an excellent seminar for anyone in the security profession 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. This seminar will also explain another aspect of security for the well rounded career security professional.

MATERIALS:

UNCLASSIFIED//FOUO w/classified discussions

PREREQ.: SECRET clearance. Also highly advisable to review ICD 704 prior to attending course.

DNI SSC ICD 704 Adjudicator Training Seminar

DNI Special Security Center

PURPOSE:

Prepare individuals 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 what goes into the adjudication process and what needs to be considered during a review to upgrade an employee to another clearance and/or access level. This is also an excellent seminar for anyone in the security profession 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. This seminar will also explain another aspect of security for the well rounded career security professional.

MATERIALS: UNCLASSIFIED//FOUO w/classified discussions

PREREQ .:

SECRET clearance. Also highly advisable to review ICD 704 prior to attending course.

DNI SSC 6/9 Physical Security Seminar

PURPOSE:

Outline 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 use of telephone and intercommunication equipment, destruction devices, TEMPEST and the threat to US systems. Attendees 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//FOUO w/classified discussions

PREREQ.: SECRET clearance. Also highly advisable to review DCID 6/9 "Manual for Physical Security

Standards for Sensitive Compartmented Facilities (SCIFs)" prior to course.

DNI SSC Government Special Security Officer Course (GSSOC)

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 (DCID 6/9)
- ★ Personnel Security (ICD 704)
- ★ Information Systems Security (DCID 6/3)
- **★** OPSEC
- ★ COMSEC
- ★ Analytic Risk Management
- ★ Security Awareness Training & Education

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

For Government Personnel only or contractors sitting in a Government position on-site and performing the SSO role (approval required)

DNI SSC Mid-Level Special Security Officer Course (MSSOC)

PURPOSE: Expose mid-level security officers to security issues and perspectives that prepare them for positions of greater responsibility in the security profession. The MSSOC is the middle step in a three level comprehensive training development hierarchy for IC Security Professionals. The MSSOC 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 from Multiple Perspectives
- ★ Communicating Security
- ★ Leading an Effective Security Organization
- ★ Managing Security as a Business
- ★ Making the Most of Your Security Career
- Spotlight Panel

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

Security professionals who administer all aspects of SCI programs TARGET:

MATERIALS: UNCLASSIFIED w/classified discussions

PREREQ .: For Government Personnel only or contractors sitting in a Government position on-site and

performing the SSO role (approval required)

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 and scenarios 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
- ★ Communication for Motivation
- ★ CI Management Responsibilities
- Ethics
- ★ Violence in the Workplace
- ★ Crisis Management and Emergency Preparedness
- ★ Security Career and Management
- ★ 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

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

This page is maintained by the DNI Special Security Center Office. If you have any questions or feedback about this site, please call the DNI Special Security Center Office at 571.204.6589

Air Army CIA USCG DIA DoE DHS DoS Treasury DEA FBI USMC NGA NRO NSA Navy Force



Home :: Community Services Division (CSD) :: Security Research Program

Organization

Chart

Community Services Division

Oversight & Liaison Division

Policy & Planning Division

CAPCO Division

SSC Portal

Joint Suitability and Security Clearance Reform Team

ODNI

Security Research Program

The SSC Research Program studies the effectiveness of personnel security programs and processes currently in place throughout the government. The Research Program examines current security procedures and concepts, proposes and test hypotheses for enhancing the future effectiveness of security and conducts a wide range of studies and other essential activities to advance the body of knowledge essential for addressing the tactical and strategic personnel security needs of the federal government.

The Research Program is currently supporting national research efforts designed to accomplish security objectives mandated in the Intelligence Reform and Terrorism Prevention Act of 2004. In that capacity, Research Program representatives are teaming with leaders from the Office of Management and Budget, the Office of Personnel Management, and representatives from all IC agencies.

This page is maintained by the DNI Special Security Center Office.





































1 of 1 7/18/2012 8:43 AM



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

SPECIAL SECURITY CENTER

Serving the Security Community

Welcome

Home :: Community Services Division (CSD) :: IC Badge Interoperability Program

Organization

Chart

Community Services

Division

Oversight & Liaison Division

Policy & Planning Division

CAPCO Division

SSC Portal

Joint Suitability and Security Clearance Reform Team

ODNI

IC Badge Interoperability Program

The DNI Special Security Center facilitates the IC Badge Interoperability Program (ICBIP). In that capacity, the SSC works closely with representatives of the National Security Agency, Central Intelligence Agency, Defense Intelligence Agency, National Geospatial Intelligence Agency and the National Reconnaissance Office to achieve badge interoperability for government and contractor personnel working in those agencies.

Badge interoperability is achieved by linking the access control systems of participating agencies over a secure SCI network. This enables badge holders from the participating agencies to use their agency-issued badge and PIN to seamlessly enter all participating agencies. The participating agencies overcame many technical challenges to integrate their disparate access control systems in order to exchange badge data over the SCI network. These systems were not intended to work together when procured by each respective agency, but the agencies and the SSC worked together to find the technical solutions to make badge interoperability a reality.

The ICBIP marks an important milestone for the Intelligence Community. It is also an accomplishment that we want to expand upon so that the rest of the Intelligence Community may share in the benefits of badge interoperability. Badge interoperability facilitates information sharing and the mobility of personnel within the agencies of the Intelligence Community. It reflects the reality of our shared mission and our need to work collaboratively to fight the global war on terrorism and to face the many new challenges of this new center

This page is maintained by the DNI Special Security Center Office.



































OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Special Security Center

Serving the Security Community

Welcome

home :: Community Services Division (CSD) :: Course Descriptions

Oganization Chart

Community

Services Division

O

Oversight & Liason Division

Policy & Planning Division

CAPCO Division

SSC Portal

Joint Suitability and Security Clearance

Reform Team

ODNI

Security Operations Curriculum Development Support Documents

PURPOSE:

To provide academic institutions with an overview of the Security Profession as it pertains to US

Government Civil Service.

BACKGROUND:

In pursuing goals associated with the Intelligence Community Five-Year Strategic Human Capital Plan, specifically being the "employer of choice able to attract and retain the very best and brightest in our ranks", the ODNI Special Security Center is pursuing the development of an academic degree that will support attracting future Security Professionals.

Security Operations is an academic area that is an amalgamation of the seven basic security disciplines—personnel security, physical security, information security, communications security, information systems security, investigations and security management. We believe it is time to join

with academe to create such a program.

TARGET:

Academic institutions who are interested in developing curriculum for a Security Operations

academic discipline specifically designed for the in-resident student.

DOCUMENTS:

Baseline Definition of the Security Profession

Security Operations Competencies: Submittal for Academic Curriculum Development

Development and Application of Skill Standards for Security Practitioners

This page is maintained by the DNI Special Security Center Office.

If you have any questions or feedback about this site, please call the DNI Special Security Center Office at 703.482.3597 (non-secure) or 93-58809 (secure).

Air Army CIA USCG DIA DoE DHS DoS Treasury DEA FBI USMC NGA NRO NSA Navy Force

1 of 1 7/18/2012 8:44 AM



Home :: Oversight and Liaison Division (O&L)

Organization

Chart

Community Services

Division

Oversight & Liaison Division

Policy & Planning Division

CAPCO Division

SSC Portal

Joint Suitability and Security Clearance Reform Team

ODNI

Oversight and Liaison Division (O&L)

The Oversight and Liaison (O&L) Division is tasked to maintain close liaison with government oversight elements. The objective of SSC is to maintain open and timely relations with all organizations working to strengthen IC security. The establishment of the SSC has allowed for the IC security oversight community to have a focal point for security matters. The O&L Division is structured in the following two branches:

The **Assessment & Liaison Branch** conducts security assessments throughout the IC for insight into security implementation, while confirming the level of compliance with existing security directives. Teams conducting on-site liaison visits also provide the latest information on new policies, confirm application of security policy and identify trends or issues that require action by the SSC. The branch can also conduct specific issue surveys, in-depth organizational-based reviews and other more detailed analyses, as needed.

The **Special Review Branch** manages the Security Incident Reporting Office, which provides guidance, oversight and conducts special inquiries in response to security incidents as required by ICD 701 (Security Policy Directive for Unauthorized Disclosure of Classified Information) and other policy. Incidents are reported to IC leaders, monitored until the investigation is completed and analyzed for trends and countermeasures. The branch also conducts related education and awareness efforts.

This page is maintained by the DNI Special Security Center Office.



































1 of 1 7/18/2012 8:45 AM



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Special Security Center

Serving the Security Community

Welcome

Home :: Community Services Division (CSD) :: Research Program

Organization

Chart

Community Services Division

Oversight & Liaison Division

Policy & Planning Division

CAPCO Division

SSC Portal

Joint Suitability and Security Clearance Reform Team

ODNI

Policy and Strategic Planning Division (P&P)

The Policy and Strategic Planning Division develops and coordinates policy and plans for the protection of sensitive compartmented information (SCI) and intelligence sources and methods. The division works closely with National Intelligence Program (NIP) agencies, non-Title 50 agencies, industry and foreign partners. The division chairs or participates on community or national-level Expert Working Groups (EWGs), creating new policies or changing existing policies and plans. The division develops IC-wide Implementation Plans with security goals, initiatives and measures in support of the National Intelligence Strategy, and establishes IC-wide programmatic guidance and priorities for all security-related programs and expenditures. The division also works with the National Security Council's (NSC) Records Access and Information Security Policy Coordinating Committee (PCC) to help develop Executive Orders and support national security policy formulation.

This page is maintained by the DNI Special Security Center Office.









































Home :: CAPCO

Welcome

Organization Chart

Community Services Division

Oversight & Liaison Division

Policy & Planning Division

CAPCO Division

SSC Portal

Joint Suitability and Security Clearance Reform Team

ODNI

Controlled Access Program Coordination Office (CAPCO)

Director of Central Intelligence Directive (DCID) 6/11 was issued in 1995 establishing the Controlled Access Program Oversight Committee (CAPOC) to assist the Director of Central Intelligence in carrying out his responsibilities for controlled access programs in the National Foreign Intelligence Program. In 2006 Intelligence Community Policy Memorandum (ICPG) 2006-700-10 established the Senior Review Group (SRG), under the direction of the CAPOC Chair, as the management body for compartmented programs under the purview of the Director of National Intelligence (DNI). These two policy documents established the Controlled Access Program Coordination Office (CAPCO) as the DNI's focal point for issues and processes dealing with controlled access programs.

The Sensitive Compartmented Information (SCI)/Special Access Program (SAP) Management (SSM) branch is the staffing element for the CAPOC and the SRG, which are responsible for oversight and management of all IC controlled access programs on behalf of the DNI. The SSM staff facilitates and participates in cross program reviews on SCI control systems, SAPs and, in conjunction with DoD♦s Special Access Program Coordination Office (SAPCO), DoD intelligence SAPs. The SSM branch coordinates with the SAPCO during the formulation of policy to ensure the maximum reciprocity of standards.

The Director of Central Intelligence Directive (DCID) 6/6 dated July 13, 2001 mandated "A uniform list of security control markings authorized for dissemination of classified information by components of the Intelligence Community, and the authorized abbreviated forms of such markings, shall be compiled in the Authorized Classification and Control Markings Register (known as the CAPCO Register) maintained by the [CAPCO] pursuant to DCID [6/11]." This system uses a uniform list of markings and provides the allowable vocabulary for all national intelligence markings and other non-IC markings applied to all media produced and collected by components of the IC, and is overseen and maintained by the Classification and Control Markings (CCM) branch. The CCM staff ensures standardization within the IC by managing and maintaining the Register and its associated Implementation Manual, and by providing advice and guidance regarding National and IC level markings standards to all elements of the IC, DoD and other users of national intelligence information. The CCM staff also manages the Classification Marking Implementation Working Group (CMIWG), active since 1998 and established by ICPG 2006-700-10 as a standing IC-wide body responsible for coordinating all changes to the CAPCO Register and Implementation Manual. The CMIWG comprises senior security policy representatives with a classification management background representing their agencies' positions on marking issues affecting the IC.

This page is maintained by the DNI Special Security Center Office.



































1 of 1 7/18/2012 8:46 AM

Intelink

Remote Access Login

Username:			
Password:			
	Log-in	Reset	

Note: The appearance of this log-in page was changed on 8 April 2011

US GOVERNMENT WARNING

WARNING! US Government (USG) computer systems are provided for the processing of official USG information only. Use of this system is restricted to authorized users. The system is monitored to ensure information security, system integrity, and the limitation of use to official purposes. The use of USG computer systems constitutes consent to monitoring as an integral part of system management. If you do not consent to monitoring or are not an authorized user of this system, exit this system now.

Visit the <u>remote access website</u> for more information about how to obtain an account. Remote Access Sessions may terminate 30 minutes after log in. Please save frequently. (AJ5)

Technical Assistance: 301-688-1800 (commercial), 644-1800 (DSN).

1 of 1 7/18/2012 8:47 AM



Organization

Chart

Community Services Division

Oversight & Liaison Division

Policy & Planning Division

CAPCO Division

SSC Portal

Joint Suitability and Security Clearance Reform Team

ODNI

Home:: Organization Chart

Joint Suitability and Security Clearance Reform Team

The Joint Suitability and Security Clearance Reform Team (Joint Reform Team) is comprised of representatives from the Office of the Director of National Intelligence (ODNI), the Department of Defense (DoD), the Office of Personnel Management (OPM), and the Office of Management and Budget (OMB), and is hosted by the Director of National Intelligence/Special Security Center (DNI/SSC).

In a memorandum dated February 5, 2008, the President requested that the Joint Reform Team provide an initial reform proposal on security clearance and suitability determinations. The goal of the proposal was to achieve government-wide improvement and streamlining of the processes for determining eligibility for access to classified information, suitability for Federal employment, and eligibility to work on a Federal contract, as well as granting access to Federally controlled facilities and information systems.

In response to the President's request, the Joint Reform Team collaborated on and submitted a Security and Suitability Process Reform Initial Report which outlines specific actions to achieve the President's goals. The report recommends primary and subordinate actions to further improve hiring and clearing processes, and proposes a new Executive Branch governance structure to ensure these processes are effectively coordinated.

Executive Order 13467, signed June 30, 2008, establishes this new governance structure by creating a Performance Accountability Council to ensure the alignment of suitability and security processes and to sustain reform momentum. Additionally, the Executive Order designates a Suitability Executive Agent and a Security Executive Agent, and grants authorities to Director of National Intelligence as the Security Executive Agent. Accordingly, the DNI has oversight authority for investigations and determinations of eligibility to classified information.

The Joint Reform Team will deliver, not later than December 2008, a detailed plan for achieving high-assurance hiring and clearing processes that are faster, more efficient, and less costly than current practices.

This page is maintained by the DNI Special Security Center Office.





































1 of 1 7/18/2012 8:47 AM