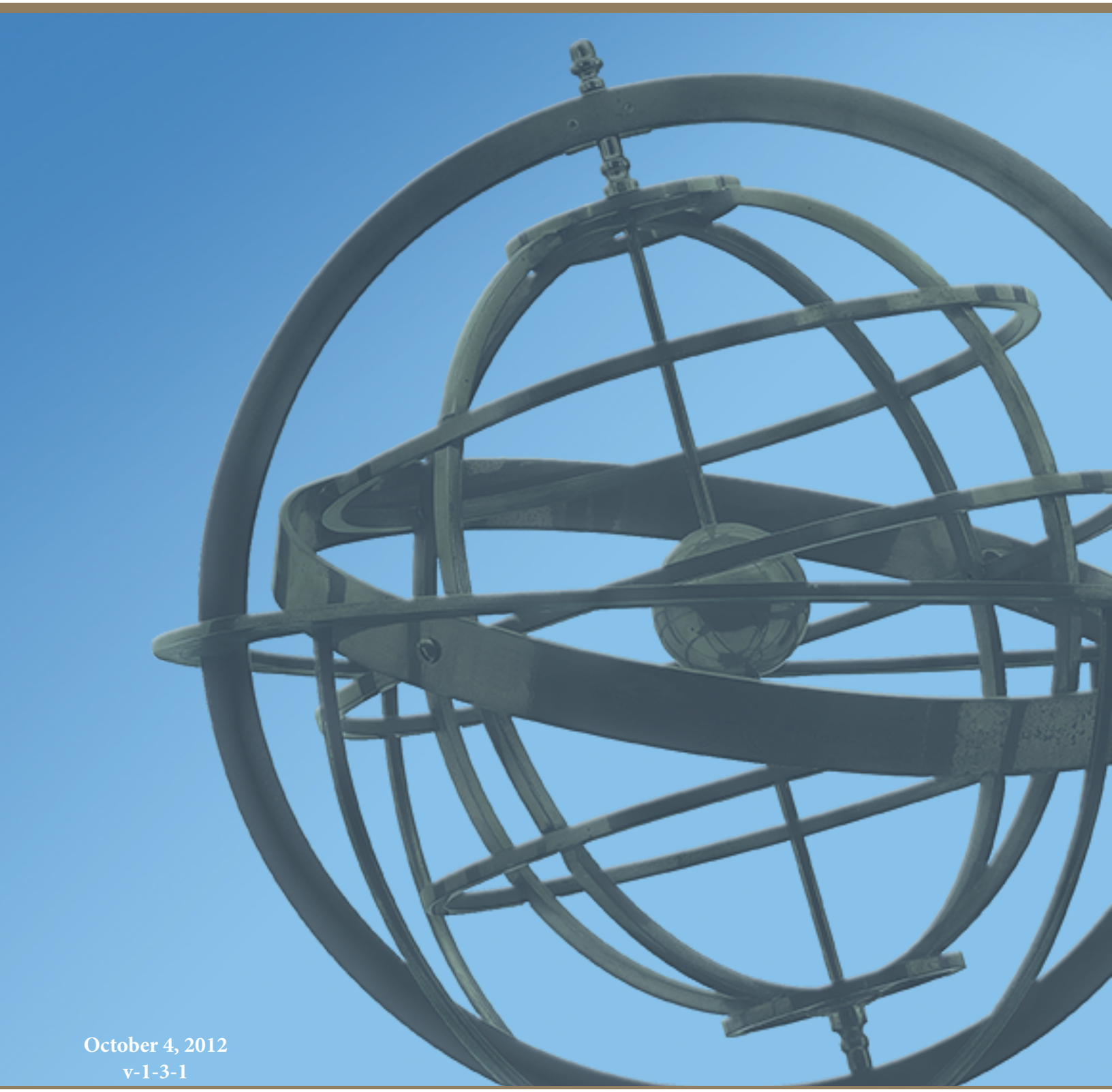
SPēD

Security Professional Education Development



October 4, 2012
v-1-3-1

Categories of

Professional Development Activities

Categories of

Professional Development Activities

TABLE OF CONTENTS

Categories of

Professional Development Activities

OVERVIEW

Security Certification Programs

A standard setting program that:

- Confers community-recognized credentials (i.e., certifications) to individuals who demonstrate mastery of a predefined set of knowledge and skills in a specified area; and
- Awards certifications only to those candidates who satisfy established criteria and/or standards by successfully meeting the requirements of a formal and standardized assessment process.

Conferees will receive 100 PDUs for each higher-level SPēD certification gained during the defined 2-year certification maintenance cycle.

Conferees will receive 45 PDUs for each approved non-SPēD, but security-focused, certification gained during a defined 2-year certification renewal cycle.

Non-Credit Bearing Training and/or Education Courses (or Certificate Programs)

A non-degree granting program that:

Consists of an organized series of planned learning experiences (instructor-led or self-paced) developed and delivered to aid participants in acquiring specific knowledge, skills, and/or competencies associated with a topic area or group of tasks that can be completed together; and

- Is delivered by an accredited training institution; and
- Awards a certificate of completion to individuals who attend and/or participate in the course.
- Conferees will receive 1 PDU for each "contact" hour (or equivalent "seat time" hour) associated with an approved non-credit-bearing training/education course or certificate program. The maximum number of allowable PDUs for each non-credit-bearing training/education course or certificate program is 45 PDUs for a defined 2-year certification renewal cycle.

Categories of

Professional Development Activities

Credit Bearing Training and/or Education Courses

A credit-bearing course that:

- Consists of an organized series of planned learning experiences (instructor-led or self-paced) designed and developed to aid participants acquire knowledge, skills, and/or competencies associated with a coherent body of study within a discipline or set of related disciplines;
- Is delivered by an accredited academic institution;
- Results in academic credits granted by and recognized by accredited academic institutions; and
- Represents a required course in an academic degree program.

Conferees will receive 15 PDUs for each credit hour of an approved credit-bearing training/education course. The maximum number of allowable PDUs for each credit-bearing training/education course is 45 PDUs for a defined 2-year certification renewal cycle.

Conferences/Workshops

A conference is a live (in-person or online) meeting with main presenter(s) to brief participants on a wide range of interrelated issues/topics.

A workshop is a working meeting or presentation with the goal of helping attendees to develop knowledge or skills associated with a specific topic area. Often includes focused exercises or collaborative work time to encourage active participation of attendees.

Conferees will receive 4 PDUs for each full day (or 2 PDUs for each half-day) of participation in an approved conference or workshop. The maximum number of allowable PDUs for participating in events in this category is 20 PDUs for a defined 2-year certification renewal cycle.

Conferees will receive an additional 3 PDUs for each unique presentation they present in an approved conference or workshop. The maximum number of allowable PDUs for presenting in events in this category is 15 PDUs for a defined 2-year certification renewal cycle.

Special Projects

Conferees may receive PDUs for successfully completing short-term special projects (i.e., SPēD Program projects) that require application of security subject matter expertise. Participation in special projects is voluntary in nature and will need to be executed outside of regular duty hours. PDUs will vary from one project to another. PDUs cannot be accrued for projects for which participation is inherently part of the participant's job and/or assigned duties.

Categories of

Professional Development Activities

RECOGNIZED LIST OF SECURITY DOMAIN-SPECIFIC PROFESSIONAL DEVELOPMENT ACTIVITIES

Security-Specific Competencies

Classification Management (Applies the requirements for classifying, marking, redacting, handling, transporting, and safeguarding protected and/or classified information)

Communications Security (Employs measures and controls to deny unauthorized persons information derived from telecommunications and ensures the authenticity of such telecommunications)

Continuity of Operations Planning (Ensures the capability exists to continue essential agency functions across a wide range of hazards, including ensuring continued performance of essential functions and succession to office of key leaders, reducing loss of life and minimizing damage, reducing or mitigating disruptions to operations, protecting essential assets, achieving a timely recovery and reconstitution, and maintaining a test, training, and exercise program for program validation)

Counterintelligence (Gathers information and conducts activities to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities)

Incident Response (Responds to crisis or urgent situations from accidents, man-made or natural disasters, or biological, chemical, radiological, or other incidents that could result in harm to people, property, or the environment. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life and preservation of property)

Information Assurance/Cyber Security (Protects the confidentiality, integrity, non-repudiation, and availability of systems, networks, and data through planning, analysis, development, penetration testing, access control, implementation, maintenance, and enhancement of information security systems, programs, policies, procedures, and tools)

Information Security (Applies knowledge of policies, procedures, and requirements established under appropriate authorities to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security)

Operations Security (Analyzes unclassified, highly sensitive, and close-hold information to identify sensitive information that could adversely affect mission if revealed to those without a need to know. Advises on the protection of the unclassified, highly sensitive, and close-hold information)

Personnel Security (Applies personnel security principles and methods to process initial clearances, periodic re-investigations, and clearance upgrades/downgrades and to complete the adjudication and appeals processes. Evaluates internal and external security clearance requests and ensures applicants' actions are consistent with regulatory requirements. Analyzes and reports on clearances and appeals findings to senior security officials and makes appropriate notifications.)

Categories of

Professional Development Activities

Security-Specific Competencies

Physical Security (Applies requirements for designing, constructing, accrediting, equipping (technically and otherwise), and securing government and contractor facilities to guard against unauthorized access. Develops and enforces access control regulations and procedures (e.g., screening and inspections))

Program Security (Employs an array of acquisition and contract security measures to sustain secrecy of highly sensitive U.S. Government programs and/or activities. Prevents unauthorized disclosure of national intelligence program information throughout the contract life cycle (e.g., FOCI; connections with adversarial or terrorist organizations))

Security Education and Training (Develops, administers, and maintains curricula and materials on the full range of security principles and practices. Conducts and tracks security and counterintelligence awareness briefings and debriefings.)

Security Program Management (Manages security implications (e.g., strategic, personnel, infrastructure, policy enforcement, emergency planning, and other resources) for a program or other area of responsibility)

Security Tools and Methods (Applies tools and methods to substantive discipline, domain, or area of work. Adapts existing tools and/or methods or employs new methodological approaches required for substantive discipline, domain, or area of work)

Vulnerabilities Assessment and Management (Conducts assessments on threats and vulnerabilities, determines the level of risk, and develops and recommends appropriate mitigation countermeasures in operational and non-operational situations. Conducts assessments in a counterintelligence context to protect against espionage, other intelligence activities, and sabotage conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities)

DOD SECURITY SPECIALIST

ABC1 - PDU 45

This entry-level course introduces the student to security disciplines, policies, procedures, and their interaction and implementation as they apply to the DoD Security Specialist career field. The course provides a common body of knowledge that promotes understanding of the scope, importance, and interdependency of the information, physical, industrial, personnel, communications, operations security programs, and other specialized areas. The course integrates programs through discussion, study, and exercises in security management, inspections and oversight, and education and training.

ID: GS101.01

Prerequisites: GS020.CU

Competencies: Classification Management, Communications Security, Information Security, Operations Security, Personnel Security, Physical Security, Program Security, Security Education and Training, Security Program Management, Security Tools and Methods, Vulnerabilities Assessment and Management

Delivery Type: Instructor-Led

Level: Introductory

Length: 8 days

Cost (Type): Yes (TDY)

Provider: DoD > DSS > CDSE

Entry Date:

Update: 02/15/2012

Link: http://www.dss.mil/cdse/catalog/classroom/GS101.html

INFORMATION SECURITY SPECIALIST CERTIFICATION (ISSC) PROGRAM

ABC2 - PDU 45

The ISSC Program is an intensive two-week training curriculum that prepares you to meet the increasing demands for skilled information technology (IT) security professionals. This certificate program integrates theoretical and practical knowledge by offering you hands-on labs combined with network design, implementation and management skills. Participants develop platform-independent expertise in securing IT systems.

Foundation in Information Security

The first week of training will focus on understanding key concepts and building critical core knowledge that will give an ISSC-certified individual the platform-independent expertise required for today's sophisticated technical environment. These concepts include understanding the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite and performing TCP and IP packets analysis. Data and communication encryption techniques and how to harden network devices and operating systems will be discussed. You will also get a practical overview of intrusion detection systems, firewalls, and other network security technologies.

Ethical Hacking 101

Advanced offensive and defensive strategies are discussed. Offensive operations include instruction and demonstrations of hands-on hacking techniques and discussions on penetration strategies with real-world examples. Defensive strategies include hardening Web servers, database systems, and operating systems to prevent unauthorized access or disclosure of sensitive data. Hands-on lab modules include popular commercial and open-source tools. You will build a hackers' toolbox you can bring back to your organization.

ID: SRTY9999T

Prerequisites: Undetermined

Competencies: Security Education and Training, Program Security, Operations Security, Information Security, Information Assurance/Cyber Security, Communications Security

Delivery Type: Instructor-Led

Level: Not Specified

Length: 10 days

Cost (Type): Yes

Provider: DOA > DOA Graduate School

Entry Date:

Update: 02/15/2012

Link: http://www.graduateschool.edu/course_details.php?cid=SRTY9999T

ARMORER CERTIFICATION COURSE

ABC3 - PDU 45

This course provides the knowledge necessary to maintain, repair, and function test standard Department of Energy (DOE) duty firearms. The Armorer Certification Program is a key part of the overall protective force mission. Armorer personnel are expected to have working-level knowledge of firearms routinely used at DOE sites. It includes a practical exercise for each firearm and written examinations, each requiring a minimum passing score of 80 percent. Upon successful completion of the course, students will be familiar with firearm characteristics, disassembly, reassembly, function testing, nomenclature, and the cycle of operation.

ID: LFR-102

Prerequisites: LFR-102R PFT-106DE

Competencies: Physical Security, Continuity of Operations Planning

Delivery Type: Instructor-Led

Level: Not Specified

Length: 80 Hours

Cost (Type): Not Specified

Provider: DOE > National Training Center

Entry Date: 07/05/2011

Update: 02/15/2012

Link: http://ntc.doe.gov/shared/courses.aspx

ARMORER RECERTIFICATION PROGRAM

ABC4 - PDU 45

This certification process provides firearms performance testing and compliance with Department of Energy (DOE) Manual 470.4-3. It is designed for active DOE Armorers holding current DOE Armorer Certification, which is nearing the expiration date. Armorers must have current factory certification for the firearms used for duty or contingency at their respective site. Recertification should be scheduled with the National Training Center Armory at least 3 months prior to the expiration date. The process itself usually takes 1 to 8 hours, depending on the number of armorers and weapon systems being taught.

ID: LFR-104

Prerequisites: LFR-102 (Armorer Certification) LFR-102R

Competencies: Physical Security, Continuity of Operations Planning

Delivery Type: Instructor-Led

Level: Not Specified

Length: 8 Hours

Cost (Type): Not Specified

Provider: DOE > National Training Center

Entry Date: 07/05/2011

Update: 02/15/2012

Link: http://ntc.doe.gov/shared/courses.aspx#PFT%20-%20Protective%20Force%20Training

FIREARMS INSTRUCTOR CERTIFICATION

ABC5 - PDU 45

This course provides instructor-level training and certification to Department of Energy (DOE) and DOE-contractor protective force personnel who are designated to conduct firearms training at DOE sites. DOE M 470.4-3A directs sites with protective force training and qualifications programs to develop and maintain instructors' qualifications and the competencies needed to perform the tasks required of the protective force training mission. This course meets the requirements for the identified instructors to accomplish this mission.

Instructor candidates will learn how to safely instruct new shooters in firearms handling and qualification courses of fire. This course addresses safety issues, detection and correction of shooter errors, range instruction, engagement simulations systems, and designing courses of fire. To successfully complete this training, instructor candidates must perform instructor candidate-directed classroom and range presentations, must pass Limited Scope Performance Tests at 100 percent, and must pass written tests at 80 percent.

MEDICAL RELEASE: Site medical clearance forms MUST be on file with the National Training Center (NTC) prior to attendance. DOE personnel must meet the medical and fitness standards mandated in 10 CFR 1046.

MANDATORY EQUIPMENT: Students must bring their site-issued duty uniforms and duty equipment, including the following: gun belt, holster, flashlight, firearms (optional), pistol and rifle, magazine pouches, knee and elbow pads, gloves (shooting), protective mask and filter with carrying pouch and billed cap. If NTC firearms are used, pre-coordination with the NTC is required.

ID: PFT-401

Prerequisites: MIT-111 (Basic Instructor Training)

Competencies: Physical Security, Continuity of Operations Planning, Incident Response

Delivery Type: Instructor-Led

Level: Not Specified

Length: 113 Hours

Cost (Type):

Provider: DOE > National Training Center

Entry Date: 07/05/2011

Update: 02/15/2012

Link: http://ntc.doe.gov/shared/courses.aspx

ADVANCED FIREARMS INSTRUCTOR CERTIFICATION

ABC6 - PDU 45

This course provides advanced instructor-level training and certification to Department of Energy (DOE) and DOE-contractor protective force personnel who are designated to conduct advanced firearms training at DOE sites. DOE M 470.4-3A directs sites with protective force training and qualifications programs to develop and maintain instructors' qualifications and the competencies needed to perform the tasks required of the protective force training mission. This course meets the requirements for the identified instructors to accomplish this mission.

AUDIENCE: DOE and DOE-contractor safeguards and security personnel responsible for advanced firearms instruction at sites with Security Police Officer (SPO) II and SPO III.

ID: PFT-401A

Prerequisites: MIT-111 (Basic Instructor Training) PFT-401 (Firearms Instructor Certification)

Competencies: Physical Security, Continuity of Operations Planning, Incident Response

Delivery Type: Instructor-Led

Level: Advanced

Length: Not Specified

Cost (Type): Not Specified

Provider: DOE > National Training Center

Entry Date: 07/05/2011

Update: 02/15/2012

Link: http://ntc.doe.gov/shared/courses.aspx

BASIC TACTICAL ENTRY INSTRUCTOR CERTIFICATION

ABC7 - PDU 45

This course covers the major elements necessary to train Tactical Entry Specialists. It addresses selection, inspection, and proper manipulation of mechanical, ballistic, and thermal breaching tools. Students will learn how to assemble a simple target folder and use it to complete a target analysis. They will also conduct classes requiring range set up, proper placement of props, and having all the proper personal protective equipment for student use. They will develop a night training exercise that will include the use of all breaching tools taught. This course includes a written exam with a minimum 80% score.

MEDICAL RELEASE: Site medical clearance forms MUST be on file with the National Training Center prior to attendance. DOE personnel must meet medical and fitness standards as mandated in Section 10 Code of Federal Regulations, Part 1046.

MANDATORY EQUIPMENT: Students must bring a load-bearing vest, knee and elbow pads, Nomex gloves, department-issued long-sleeve shirt and long pants (Nomex flight suit recommended), leather above-the-ankle boots, approved eye protection, site-issued body armor, and tactical gear with helmet.

Note: Dependent upon class size, some training days may run longer than stated in course schedule.

ID: PFT-406

Prerequisites: MIT-111 (Basic Instructor Training) PFT-405 (Basic Tactical Entry)

Competencies: Physical Security, Continuity of Operations Planning

Delivery Type: Instructor-Led

Level: Introductory

Length: 40 Hours

Cost (Type):

Provider: DOE > National Training Center

Entry Date: 07/06/2011

Update: 02/15/2012

Link: http://ntc.doe.gov/shared/courses.aspx

LIVE FIRE SHOOT HOUSE INSTRUCTOR CERTIFICATION

ABC8 - PDU 45

This is a certification demonstrating that individuals are capable of full and safe performance as lead/control instructors in the Live Fire Shoot House at their sites.

After completing PFT-407, Security Police Officer III Instructor Certification or TRF-420, Tactical Response Force Instructor Certification, individuals serve as assistant Live Fire Shoot House (LFSH) instructors under the lead/control instructor at their site. This apprenticeship satisfies the 40-hour specification in Department of Energy M 470.4-3. The lead/control instructor must determine when the apprentice is capable of full and safe performance and he or she must pass the written examination and limited scope performance testing (LSPT) at 100%. Instructors satisfying these requirements must formally request LFSH Intelligence Community certificates from the Director of the National Training Center. Documents supporting completion of above requirements must also be provided at the time of the request. Certificates will not be issued for LFSH IC unless this supporting documentation is provided.

ID: PFT-501

Prerequisites: MIT-111 (Basic Instructor Training) PFT-310 PFT-401 (Firearms Instructor Certification) TRF-420 (Tactical Response Force 2 Instructor Certification)

Competencies: Physical Security, Continuity of Operations Planning

Delivery Type: Instructor-Led

Level: Advanced

Length: 8 Hours

Cost (Type): Not Specified

Provider: DOE > National Training Center

Entry Date: 07/05/2011

Update: 02/15/2012

Link: http://ntc.doe.gov/shared/courses.aspx

TACTICAL RESPONSE FORCE (TRF) 1 INSTRUCTOR CERTIFICATION

ABC9 - PDU 45

This course provides students with instructor-level training and certification for the Department of Energy (DOE) Security Protection Officer II (SPO II) positions. Instruction includes training design of recapture/recovery support operations, set up, safety concerns, conduct of training, student debrief and evaluation. Student activities will include: lecture/ briefs, dry/live fire training in the following subjects: Live Fire Obstacle Course, Vehicle Mounted/Dismounted Fighting, Building Searches, ESS, Dynamic Entry Open/Closed Doors, Diversionary Devices. Instructor-candidates will conduct these lectures and activities under the supervision of the Live Fire Range Security Operations instructional staff and be given immediate feedback in regard to presentation and the overall effectiveness of the training delivered. Instructor candidates will be tested (pass/fail) on limited scope performance tests (LSPTs), take one written examination requiring an 80% minimum score, and pass the TRF Combined Firearms Qualification with a minimum 80% score.

MEDICAL RELEASE: Site medical clearance forms MUST be on file with the National Training Center prior to attendance. Department of Energy personnel must meet medical and fitness standards as mandated in section 10 Code of Federal Regulations, Part 1046. A valid driver's license is required for participation in the vehicle mounted/dismounted fighting.

MANDATORY EQUIPMENT: Students must bring all SPO II duty equipment, gas mask, tactical flashlight, Nomex gloves, and seasonal outdoor gear.

AUDIENCE: DOE and DOE contractor protective force personnel.

Note: Dependent upon class size, some training days may run longer than stated in course schedule.

ID: PFT-140

Prerequisites: MIT-111 (Basic Instructor Training) PFT-401 (Firearms Instructor Certification) PFT-401A (Advanced Firearms Instructor Certification) TRF-100 (Tactical Response Force 1)

Competencies: Continuity of Operations, Physical Security, Security Education and Training

Delivery Type: Instructor-Led

Level: Not Specified

Length: 80 Hours

Cost (Type): Not Specified

Provider: DOE > National Training Center

Entry Date: 07/06/2011

Update: 02/15/2012

Link: http://ntc.doe.gov/shared/courses.aspx

TACTICAL RESPONSE FORCE (TRF) 2 INSTRUCTOR CERTIFICATION

ABC10 - PDU 45

This course provides instructor-level training and certification to Department of Energy (DOE) and DOE-contractor protective force personnel who are designated to conduct TRF-200 training at DOE facilities.

DOE O 473.3, Protection Program Operations, directs sites with protective force training and qualifications programs to develop and maintain instructors' qualifications and the competencies needed to perform the tasks required of the protective force training mission. This course meets the requirements for the identified instructors to accomplish this mission.

TRF-420 addresses methods for teaching close quarters marksmanship with handgun and rifle; close quarters battle techniques; mounted, dismounted, and urban movement techniques; a variety of assault options; and mechanical and ballistic breaching techniques.

ID: TRF-420

Prerequisites: MIT-111 (Basic Instructor Training) PFT-401 (Firearms Instructor Certification)

FT-401A (Advanced Firearms Instructor Certification) PFT-405 (Basic Tactical Entry) PFT-406 (Basic Tactical Entry Instructor Certification) TRF-200 (Tactical Response Force 2)

Competencies: Physical Security, Continuity of Operations Planning

Delivery Type: Instructor-Led

Level: Not Specified

Length: 80 Hours

Cost (Type): Not Specified

Provider: DOE > National Training Center

Entry Date: 07/06/2011

Update: 02/15/2012

Link: http://ntc.doe.gov/shared/courses.aspx#PFT%20-%20Protective%20Force%20Training

SECURITY ASSET PROTECTION PROFESSIONAL CERTIFICATION (SAPPC)

C1 - PDU 100

The SAPPC serves as a valid indicator of a security practitioner's ability to apply foundational security concepts, principles, and practices the DoD community deems critical to successfully perform functions, implement programs, and pursue missions necessary to manage risks to and protect DoD assets. SAPPC asks individuals to demonstrate the application of foundational security concepts, principles, and practices.

ID: SAPPC (SPēD Program)

Prerequisites: SFPC

Competencies: Classification Management, Communications Security, Counterintelligence, Incident Response, Information Assurance/Cyber Security, Information Security, Operations Security, Personnel Security, Physical Security, Program Security, Security Education and Training, Security Program Management, Security Tools and Methods, Vulnerabilities Assessment and Management

Delivery Type: Proctored Examination

Level: Intermediate

Length: 10 days

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/27/2011

Update: 02/15/2012

Link: http://www.dss.mil/seta/sped/types-sappc.html

ANTITERRORISM OFFICER (ATO) LEVEL II

T/E1 - PDU 13.5

This course provides students with the appropriate background, skills, and abilities to qualify as an ATO for a command or organization. The course examines ATO roles and responsibilities, vulnerability and threat assessments, creating and executing antiterrorism (AT) programs, preparing AT plans, resource management, and AT training. Successful completion of this course qualifies individuals to conduct Level 1 AT briefings.

ID: GS109.16

Prerequisites: None

Competencies: Physical Security, Vulnerabilities Assessment and Management

Delivery Type: Web-Based Training

Level: Intermediate

Length: 13.5 Hours

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date:

Update: 03/28/2012

Link: http://www.dss.mil/cdse/catalog/curricula/GS109.html

DNI/SSC ICD 705 PHYSICAL SECURITY COURSE

T/E2 - PDU 40

This course prepares students to implement the construction and security protection standards required for all facilities where Sensitive Compartmented Information or Special Access Program material may be stored, used, discussed, and/or processed.

ID: FT105.01

Prerequisites: None

Competencies: Physical Security, Vulnerabilities Assessment and Management

Delivery Type: Instructor-Led

Level: Intermediate

Length: 5 Days

Cost (Type): Yes (TDY)

Provider: DoD > DSS > CDSE

Entry Date:

Update: 02/15/2012

Link: http://www.dss.mil/cdse/catalog/physical-security.html

COMPUTER NETWORK INVESTIGATIONS TRAINING PROGRAM

T/E3 - PDU 45

The CNITP is designed to train criminal investigators (or those that routinely serve as part of the investigative team) to identify, search, seize, and analyze magnetic media in a network environment. Investigators are routinely finding that the evidence they need in the furtherance of any investigation may be found on servers regardless of the type of investigation they are conducting. The purpose of this course is to give investigators an understanding of how to identify the server software in question, navigate this system, and collect evidence in a forensically sound manner. The software and hardware issued during CNITP has been researched and tested in the classroom and in the field. Students will be trained on the use of this equipment during class. During CNITP students will be issued the following computer hardware and software items which they will take with them upon completion of the course:

* MacBook Pro 15" laptop computer
* USB External hard disk
* Paraben Network Email Examiner
* F-response
* Windows 7 Professional
* Windows Server 2008 R2 Book
* VMware Fusion
* Windows Network Forensics and Investigations - Book

ID: CNITP

Prerequisites: Seized Computer Evidence Recovery Specialist (SCERS) Training Program - recommended

Competencies: Information Security, Vulnerabilities Assessment and Management, Incident Response

Delivery Type: Instructor-Led

Level: Not Specified

Length: 76 Hours

Cost (Type):

Provider: DHS > FLETC

Entry Date: 06/24/2011

Update: 02/15/2012

Link: http://www.fletc.gov/training/programs/technical-operations-division

DIGITAL EVIDENCE ACQUISITION SPECIALIST TRAINING PROGRAM

T/E4 - PDU 45

The primary purpose of the DEASTP course is to equip criminal investigators with the knowledge, skills, and abilities to properly identify and seize digital evidence. Through a combination of lecture, demonstration, hands-on exercises, labs, and a practical exercise, investigators learn how to seize digital evidence from personal computer (PC) and notebook computer hard drives, floppy diskettes, compact disks (CDs), DVDs, thumb drives, and various flash media by acquiring forensically valid images of the digital media. Investigators also learn how to preview digital media prior to acquisition to determine if the media contains key text strings, unlawful graphics, etc. The DEASTP program is an intense course that requires substantial computer aptitude. Successful completion of a graded practical exercise is required for graduation. At the conclusion of the training program, the participants will be able to successfully seize digital evidence. This knowledge will be demonstrated through the completion of an 8-hour practical exercise on the last full day of the training program. The practical exercise includes a simulated search warrant scenario. [Note: The search warrant scenario does not include tactics (dynamic building entry, handcuffing suspects, use of firearms, etc.)]. The practical exercise requires each student to work independently to acquire various types of digital evidence in a forensically sound manner. It is recommended that you attend this course before attending the Seized Computer Evidence Recovery Specialist (SCERS) training program. SCERS students are required to possess the skills and technical information presented in this course before they attend the SCERS training program.

ID: DEASTP

Prerequisites: Functional knowledge of computers

Competencies: Information Assurance/Cyber Security

Delivery Type: Instructor-Led

Level: Not Specified

Length: 76 Hours

Cost (Type): Not Specified

Provider: DHS > FLETC

Entry Date: 06/24/2011

Update: 02/15/2012

Link: http://www.fletc.gov/training/programs/technical-operations-division

INTERNET INVESTIGATIONS TRAINING PROGRAM

T/E5 - PDU 40

Investigating the cyber criminal can be one of the most complex tasks facing the law enforcement professional today and requires a multidisciplinary approach supported by technical expertise that was not needed with traditional crime. The IITP will focus on investigations and operations centered on the use of the Internet and its many communities that are being exploited for criminal activity day to day. The IITP will give the criminal investigator or analyst, the basic understanding they need to conduct cyber-based investigations.

ID: IITP

Prerequisites: Working knowledge of computers

Competencies: Information Assurance/ Cyber Security, Incident Response Vulnerabilities Assessment and Management

Delivery Type: Instructor-Led

Level: Not Specified

Length: 5 days

Cost (Type): Not Specified

Provider: DHS > FLETC

Entry Date: 06/24/2011

Update: 03/28/2012

Link: http://www.fletc.gov/training/programs/investigative-operations-division

OPSEC FOR PUBLIC SAFETY AGENCIES COUNTERTERRORISM TRAINING PROGRAM

T/E6 - PDU 24

Criminals and terrorists are becoming increasingly effective in collecting intelligence against U.S. agencies and corporations. To be successful, they need specific information about personnel, response plans, capabilities, and infrastructures. Operations Security (OPSEC) is a five-step risk management tool used by security professionals and the military that public safety agencies could use to deny our adversaries the sensitive information they need to plan their crimes and attacks. The OPSACTP is designed for public safety and special operations teams such as hazmat/weapons of mass destruction (WMD), bomb squads, tactical teams, arson and gang investigations, and the like. The OPSACTP teaches public safety officers from the law enforcement, fire- rescue, Emergency Medical Services (EMS), and emergency management communities how to use OPSEC to protect you, your mission, and your family. Students who successfully complete this training will be able to apply OPSEC to emergency and special event planning; special operations such as Special Weapons and Tactics (SWAT), HazMat, WMDs, bomb squad; intelligence, counter terrorism, arson, and narcotics task forces; and criminal investigations.

ID: DHS-002-PREV

Prerequisites: Non-credentialed students must have the permission of the OPSACTP Program Coordinator

Competencies: Operations Security, Counterintelligence, Incident Response, Vulnerabilities Assessment and Management

Delivery Type: Residential Training

Level: Not Specified
Length: Not specified
Cost (Type): No
Provider: DoD > AFOSI
Entry Date: 07/06/2011
Update: 02/15/2012

Link: https://www.rkb.us/trainingdetail.cfm?training_id=167&query=&overridesubtype=1097

PHYSICAL SECURITY TRAINING PROGRAM

T/E7 - PDU 45

The Physical Security training Program (PSTP) is a basic physical security training program designed to provide baseline knowledge of physical security systems and procedures. The survey process is the common thread used in teaching this program. The PSTP includes conceptual security considerations, vulnerabilities assessments, and familiarization with hardware and procedures. A comprehensive practical exercise is followed by a formal presentation of the survey results by each of the survey groups.

ID: PSTP

Prerequisites: None

Competencies: Physical Security, Vulnerabilities Assessment and Management

Delivery Type: Instructor-Led

Level: Not Specified
Length: 10 Days
Cost (Type): Not Specified
Provider: DHS>FLETC
Entry Date: 06/24/2011
Update: 02/15/2012

Link: http://www.fletc.gov/training/programs/counterterrorism-division

(DNI/SSC) 6/9 PHYSICAL SECURITY SEMINAR

T/E8 - PDU 38.5

This course outlines the construction and security protection standards required for all U.S. Government facilities or U.S. 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 U.S. systems. Attendees discuss current physical security concerns of their respective organizations and brainstorm solutions.

ID: Not Specified

Prerequisites: SECRET Clearance

Competencies: Physical Security, Vulnerabilities Assessment and Management

Delivery Type: Instructor-Led

Level: Not Specified

Length: 5 Days

Cost (Type): Tuition-Free

Provider: DoD > DNI Special Security Center

Entry Date: 06/24/2011

Update: 03/27/2012

Link: http://cryptome.org/2012/07/dni-ssc.pdf

DNI/SSC SENSITIVE CLASSIFIED INFORMATION (SCI) OVERVIEW SEMINAR (PARTS 1, 2, & 3)

T/E9 - PDU 3 (each)

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: Highlights key security points from Part 1, and provides 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: 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.

ID: Not Specified

Prerequisites: TS/SCI & have signed the NDA for parts 1 and 2.

Competencies: Information Security, Operations Security

Delivery Type: Instructor-Led

Level: Not Specified

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

Cost (Type): Tuition-Free

Provider: DoD>DNI> DNI Special Security Center

Entry Date: 06/24/2011

Update: 02/15/2012

Link: http://www.graduateschool.edu/course_details.php?cid=SRTY7030A

DNI/SSC LIFE IN A SCIF

T/E10 - PDU 17

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.

ID: Not Specified

Prerequisites: Attendees must have TS/ SCI

Competencies: Information Security, Operations Security

Delivery Type: Instructor-Led

Level: Not Specified

Length: 2 days

Cost (Type): Tuition-Free

Provider: DoD>DNI>DNI Special Security Center

Entry Date: 06/27/2011

Update: 03/27/2012

Link: http://cryptome.org/2012/07/dni-ssc.pdf

DNI/SSC MID-LEVEL SPECIAL SECURITY OFFICER COURSE

T/E11 - PDU 38.5

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

ID: MSSOC

Prerequisites: N/A

Competencies: Security Program Management, Operations Security, Information Security

Delivery Type: Web-Based

Level: Intermediate

Length: 5 days

Cost (Type): Tuition-Free

Provider: DoD > DNI > DNI Special Security Center

Entry Date: 06/27/2011

Update: 03/27/2012

Link: http://cryptome.org/2012/07/dni-ssc.pdf

DNI/SSC SENIOR SECURITY PROFESSIONAL SEMINAR (SSPS)

T/E12 - PDU 40

This seminar will 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
* Counterintelligence (CI) Management Responsibilities
* Ethics
* Violence in the Workplace
* Crisis Management and Emergency Preparedness
* Security Career and Management
* Spotlight Panel (security leaders from different Intelligence Community (IC) agencies)
* Keynote guest speakers from different IC agencies

ID: SSPS

Prerequisites: GS 14-15 or equivalent; minimum 10 years security experience

Competencies: Security Program Management, Continuity of Operations Planning

Delivery Type: Instructor-Led

Level: Advanced

Length: 5 Days

Cost (Type): Tuition-Free

Provider: DoD > DNI > DNI Special Security Center

Entry Date: 06/27/2011

Update: 02/15/2012

Link: http://cryptome.org/2012/07/dni-ssc.pdf

DNI/SSC ICD 704 ADJUDICATOR TRAINING SEMINAR (FORMERLY DCID 6/4)

T/E13 - PDU 38.5

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.

ID: Not Specified

Prerequisites: SECRET Clearance

Competencies: Physical Security, Operations Security

Delivery Type: Instructor-Led

Level: Not Specified

Length: 5 Days

Cost (Type): Tuition-Free

Provider: DoD > DNI Special Security Center

Entry Date: 06/27/2011

Update: 03/27/2012

Link: http://cryptome.org/2012/07/dni-ssc.pdf

DNI/SSC GOVERNMENT SPECIAL SECURITY OFFICER COURSE (GSSOC)

T/E14 - PDU 38.5

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)
* Operations Security
* Communications Security
* Analytic Risk Management
* Security Awareness Training & Education

ID: GSSOC

Prerequisites: TS/SCI and 2-5 years' security experience

Competencies: Physical Security, Personnel Security, Information Security, Operations Security, Communications Security, Incident Response, Security Awareness Training & Education

Delivery Type: Instructor-Led

Level: Not Specified

Length: 5 days

Cost (Type): Tuition-Free

Provider: DoD>DNI> DNI Special Security Center

Entry Date: 06/27/2011

Update: 03/27/2012

Link: http://cryptome.org/2012/07/dni-ssc.pdf

INTERNATIONAL SECURITY AND TECHNOLOGY TRANSFER/CONTROL

T/E15 - PDU 40

This course teaches students to identify, analyze, and apply the laws, policies, and processes that govern International Security and Technology Transfer/Control. The course characterizes national security policy issues and export/import licensing constraints (as defined by the Departments of State, Commerce, and Treasury) and guides evaluating their effects on domestic and international DoD programs. Students will learn the procedures for the export and import of defense and dual-use equipment and services, for handling classified and controlled unclassified program information, and for foreign visit control. Students will learn to recognize hostile and friendly foreign power elicitation and technology collection methods and techniques and develop methods of protecting information. Students will also learn to describe the U.S. Government's ownership, usage, and transfer rights of intellectual property to foreign governments and contractors.

ID: PMT 203

Prerequisites: CLI 007, Technology Transfer and Export Control

Competencies: Information Security, Operations Security

Delivery Type: Instructor-Led

Level: Not Specified

Length: 2 Days

Cost (Type): Not Specified

Provider: DoD>DAU

Entry Date: 06/27/2011

Update: 03/27/2012

Link: http://icatalog.dau.mil/onlinecatalog/courses.aspx?crs_id=54

OVERHEAD MANAGEMENT OF DEFENSE CONTRACTS

T/E16 - PDU 45

Overhead Management of Defense Contracts provides an understanding of industry overhead costs and the costs' impact on seller pricing/business strategies under various acquisition environments with differing contract types. Attendees will understand the development and application of overhead rates used in contract formation, administration, and closeout. The course-integrating case study provides hands-on application of the overhead-rate process in which attendees determine their own final overhead rates.

ID: CON 232

Prerequisites: CON 280, Source Selection and Acquisition of Service Contracts
CON 290, Contract Administration and Negotiation Techniques in a Supply Environment

Competencies: Program Security, Security Program Management

Delivery Type: Instructor-Led

Level: Not Specified
Length: 10 Days
Cost (Type): Not Specified
Provider: DoD>DAU
Entry Date: 06/24/2011
Update: 03/27/2012

Link: http://icatalog.dau.mil/onlinecatalog/courses.aspx?crs_id=27

ADVANCED INTERNATIONAL MANAGEMENT WORKSHOP

T/E17 - PDU 40

This course is designed to prepare professionals to participate effectively in the development and negotiation of defense armaments cooperation agreements ranging from simple data exchange annexes to complex cooperative development, production, and support agreements. Students who successfully complete this course will be able to synthesize, integrate, and apply U.S. policy on international cooperative defense acquisition, including policies of the Departments of Defense, State, Commerce, and Treasury. The final outcome of the week is formulating and practicing negotiation of international acquisition agreements in accordance with U.S. policies, statutes, and regulations.

ID: PMT 304

Prerequisites: PMT 202, Multinational Program Management
PMT 203, International Security and Technology Transfer/Control
PMT 202, Multinational Program Management
PMT 203, International Security and Technology Transfer/Control

Competencies: Program Security, Security Program Management

Delivery Type: Instructor-Led

Level: Not Specified
Length: 5 Days
Cost (Type): Not Specified
Provider: DoD>DAU
Entry Date: 06/27/2011
Update: 03/27/2012

Link: http://icatalog.dau.mil/onlinecatalog/courses.aspx?crs_id=58

INTERNATIONAL PROGRAMS SECURITY REQUIREMENTS COURSE

T/E18 - PDU 24

The International Programs Security Requirements course covers the principles and procedures that facilitate international technology transfer, export controls, and foreign disclosure. Specific lessons discuss the acquisition process for international program security, controlled unclassified and foreign government information the National Disclosure Policy and the International Traffic in Arms Regulations (ITAR). The export approval and license process is covered along with the role of the Defense Security Service (DSS). Other topics include visits and assignments of foreign nationals, Multinational Industrial Security Working Group (MISWG) documents, Committee on Foreign Investment in the United States (CFIUS) and Foreign Ownership, Control or Influence (FOCI), and the transfer of classified information.

ID: IPSR

Prerequisites: None

Competencies: Program Security, Security Program Management, Operations Security, Communications Security

Delivery Type: Instructor-Led

Level: Not Specified

Length: 3 Days

Cost (Type): Not Specified

Provider: DoD Defense Institute of Security Assistance Management

Entry Date: 06/27/2011

Update: 02/16/2012

Link: http://www.disam.dsca.mil/pages/courses/onsite/ipsr3.aspx?tab=des

SECURITY COOPERATION MANAGEMENT TRAINING OFFICER/TRAINING MANAGER COURSE

T/E19 - PDU 40

The TO course provides a comprehensive overview of Security Cooperation (SC) and Security Assistance (SA) management, and the interrelationships of the IMSO and the international student. The curriculum explores Security Cooperation legislation, human rights considerations, SC/SA organizations and functions, and SC/SA planning and programming. In addition, the curriculum examines the individual elements of the DoD Field Studies Program (DoD FSP), Invitational Travel Orders (ITO), International Military Student's legal status, International Military Students' health entitlements while attending SC/SA training, and use of the Security Assistance Network (SAN) and the IMSO Web. The curriculum further provides a review of Service-unique: organizations, student administration procedures, training program automation, DoD FSP presentation practices and funding, and a comprehensive survey of cross-cultural considerations that impact the IMSO-IMS environment.

The TM Course presents a survey of the wide variety and principle features of Security Cooperation/Security Assistance Legislation and Policy, introduces the student to the role of the SCO in support of U.S. national security strategy and other supporting DoD and DoS strategic guidance, and examines the various Security Cooperation planning documents and processes for the execution of SC – with emphasis on International Military Training and the Combined Education and Training Program Plan (CETPP). The TM course also provides an overview of the entire life cycle of an FMS case with particular emphasis on international training, and financial management regulations that determine tuition pricing for International Military Training.

Note: TM students who complete the classroom portion of this course but do not complete the TM distance learning pre-requisite by day 3 of class will receive a TO certificate in lieu of a TM certificate.

ID: SCM-TO/TM

Prerequisites: CLI 007, Technology Transfer and Export Control

Competencies: Program Security, Security Program Management

Delivery Type: Instructor-Led

Level: Not Specified

Length: 5 Days

Cost (Type): Not Specified

Provider: DoD Defense Institute of Security Assistance Management

Entry Date: 06/27/2011

Update: 02/16/2012

Link: http://www.disam.dsca.mil/pages/courses/onsite/scm-to.aspx

SECURITY COOPERATION MANAGEMENT OVERSEAS COURSE

T/E20 - PDU 45

Instruction is provided on the many complex and interrelated aspects of security assistance and security cooperation. These include the role of the Department of State in foreign policy, that of the Department of Defense in national defense, and that of the Congress in the areas of authorization, appropriation, and oversight. The functions and responsibilities of the geographic combatant commands (GCCs), the Defense Security Cooperation Agency (DSCA), and the Military Departments are also addressed. The syllabus (below) lists the various topics covered in this course. The emphasis of the curriculum is on the policies and procedures involved in the operational management of security assistance and security cooperation activities in an overseas environment. Associated studies include cross-cultural communications, anti-terrorism and force protection, human rights, management of budget and other resources within the Security Cooperation Organization (SCO), various automation programs, and international training management responsibilities. The course includes practical exercises and computer labs with typical scenarios for SCO personnel.

The curriculum also includes a regional studies program directed by DISAM area specialists. This covers regional and country-specific political, military, economic, geographic, and cultural considerations, plus historic and current relationships with the U.S. For this part of the curriculum, students are divided into five regional seminars – Europe, Africa, Middle East, Western Hemisphere, and the Asia-Pacific region, which generally matches the areas of responsibility of the GCCs. The regional studies seminars utilize presentations by guest lecturers from U.S. Government agencies, civilian universities, and private organizations, as well as by Defense Institute of Security Assistance Management (DISAM) faculty members.

Selected students identified by the gaining GCC and/or SCO will receive additional instruction, known as specialized training, in some or all of the following areas: international training management, SCO resource management, armaments cooperation, and international logistics; there are a total of eight blocks of specialized training.

ID: SCM-O

Prerequisites: Students are required to complete one or both of two online lessons prior to reporting to DISAM. These can be found at this

* SCO Overseas Entitlements
* Ethics and Standards of Conduct

Each lesson should take approximately 1 hour to complete.

Competencies: Program Security, Security Program Management

Delivery Type: Instructor-Led

Level: Not Specified

Length: 15-19 days

Cost (Type): Not Specified

Provider: DoD Defense Institute of Security Assistance Management

Entry Date: 06/27/2011

Update: 03/27/2012

Link: http://www.disam.dsca.mil/pages/courses/onsite/scm-o.aspx?tab=des

SECURITY COOPERATION MANAGEMENT PROGRAM AND CASE MANAGEMENT COURSE

T/E21 - PDU 40

The course encompasses a broad variety of topics involved in total package support of international programs. Topics include pertinent applications of the Arms Export Control Act and other statutory requirements, Department of Defense (DoD) and Service-implementing directives and instructions, Foreign Military Sales (FMS) policy directives and program requirements, and Security Cooperation (SC) automated information systems. The course emphasizes effective use of FMS organizational relationships among DoD acquisition, logistical, financial, and case management personnel. The SAM-CM course will provide SC personnel with an increased knowledge of FMS policies, procedures and systems. The goal is to provide new perspectives on effective case management methodologies. To a large extent, this goal is met through the discussion of current event issues, sample case management problems and military department (MILDEP)-unique seminars. Whenever possible, guest speakers from the Defense Security Cooperation Agency and the MILDEPs are used to enhance the current issues and policies discussions. Click on Continuous Learning Points for the SAM-CM course for Acquisition and other Professional Development Program points which can be acquired.

ID: SCM-CM

Prerequisites: N/A

Competencies: Program Security, Security Program Management

Delivery Type: Instructor-Led

Level: Not Specified

Length: 5 Days

Cost (Type): Not Specified

Provider: DoD Defense Institute of Security Assistance Management

Entry Date: 06/27/2011

Update: 02/16/2012

Link: http://www.disam.dsca.mil/pages/courses/onsite/scm-cm.aspx

SECURITY COOPERATION MANAGEMENT CONUS COURSE

T/E22 - PDU 40

The SCM-C Course consists of completing the Security Cooperation Orientation and International Programs Security Requirements (IPSR) Courses, (see Prerequisites below), and classroom lessons. The on-line portion (SCM-OC-OL) is a series of lessons taken by students at their own pace during a 60 day period that starts no earlier than 70 days, and ends no later than 10 days prior to the classroom portion of the Course. If a student completes SCM-OC-OL more than 70 days prior to the first day of class, they will be required to retake SCM-OC-OL within the prescribed window. The 10 day window prior to the start of the classroom portion of the Course is to ensure all students have completed the SCM-OC-OL Course and to prepare orders so students may attend the classroom portion of the Course.

Students must successfully complete all lessons and quizzes in SCM-OC-OL during the prescribed time period or they will not be allowed to attend the classroom portion of SCM-C. Each on-line block will cover either a specific functional area of Security Cooperation, like Training, or multiple sub-blocks will cover some of the larger areas, like Logistics. SCM-OC-OL lessons may be completed at one time or you may start and stop at different points in the lesson and resume your study at a later time. There are quizzes at the end of each block of SCM-OC-OL, and daily take home quizzes during SCM-C. SCM-OC-OL blocks must be reviewed and all exams passed with a grade of 100% before a student may enroll in the resident portion of the SCM-C Course. If a student receives a grade of less than 100% on an online quiz a new quiz will be given until a score of 100% is achieved. A score of 70% is required for the daily take home quizzes in SCM-C. SCM-C (classroom) lessons will be blocks of exercises that reinforce the on-line lessons, and will simulate actual procedures, decision trees, work flows and problems associated with Security Cooperation. The classroom portion of the Course is one week (5 days) long. Topics addressed include legal foundations, technology transfer, program planning and coordination, program security, acquisition, contracting, financial management, logistics, training, management documentation and Security Cooperation Information Portal.

ID: SCM-C

Prerequisites: ISPR

Competencies: Security Program Management

Delivery Type: Web-Based Training & Instructor-Led

Level: Not Specified

Length: 5 Days

Cost (Type): Not Specified

Provider: DoD Defense Institute of Security Assistance Management

Entry Date: 06/27/2011

Update: 02/16/2012

Link: http://www.disam.dsca.mil/pages/courses/onsite/scm-c.aspx#dat

SECURITY COOPERATION MANAGEMENT USG EXECUTIVE AND U.S. DEFENSE INDUSTRY COURSE

T/E23 - PDU 40

SCM-E curriculum encompasses a broad range of SC and SA related topics as described in the course syllabus below. The course is intended for U.S. personnel who now occupy (or have been selected to occupy) executive Security Cooperation management positions within the Department of Defense (DoD). It is also intended for defense industry personnel who are currently occupying positions in international sales or related positions in financial management, international logistics, operations, or customer support. Persons in related positions in other federal agencies, such as the Department of State (DoS), may also attend this course. Click on Continuous Learning Points for the SCM-E course for Acquisition and other Professional Development Program points which can be acquired.

ID: SCM-E

Prerequisites: N/A

Competencies: Security Program Management

Delivery Type: Web-Based Training & Instructor-Led

Level: Advanced

Length: 5 Days

Cost (Type): Yes

Provider: DoD Defense Institute of Security Assistance Management

Entry Date: 06/27/2011

Update: 02/16/2012

Link: http://www.disam.dsca.mil/pages/courses/onsite/scm-e.aspx

SECURITY COOPERATION MANAGEMENT LOGISTICS SUPPORT COURSE

T/E24 - PDU 40

This is an advanced course in two parts. The first part is an online refresher course. The second part is a one-week resident course. The online refresher course should be completed no more than 60 days prior to the start of the resident course. Students should already have attended an introductory course and be familiar with FMS programs and procedures. The course focuses on specific aspects of logistics such as the integration of the elements of the total package approach, requirements determination, requisition processing, with an emphasis on shipping and transportation considerations throughout the FMS case and requisition life cycle. The course emphasizes the responsibilities and relationships between the case managers at the ILCOs with the weapon system program manager, the contract administrative office, the DLA and military department (MILDEP) item managers, the transportation coordinators, the freight forwarder, and the FMS customer. The course will focus on how to reduce frustrated and misdirected shipments, reduce supply discrepancy reports, and plan for material movement during LOR development. Click on Continuous Learning Points for the SCM-CS Logistics Support Course for acquisition and other professional development program points which can be acquired. Students are required to complete an online refresher course prior to being accepted for registration, and must pass a final examination at the end of the course with a minimum score of 75 percent to receive a certificate of graduation for SCM-CS Logistics Support Course

ID: SCM-CS

Prerequisites: Minimum of 1 year of working experience in a security cooperation position, or 1 year of performing logistics functions related to security cooperation. Graduation from a basic introductory DISAM course is a prerequisite.

Competencies: Security Program Management

Delivery Type: Instructor-Led

Level: Advanced

Length: 5 Days

Cost (Type): Yes

Provider: DoD Defense Institute of Security Assistance Management

Entry Date: 06/27/2011

Update: 02/16/2012

Link: http://www.disam.dsca.mil/pages/courses/onsite/scm-cs.aspx

FINANCIAL MANAGEMENT COURSE

T/E25 - PDU 40

The course encompasses a broad variety of topics, including the Arms Export Control Act and other statutory requirements; Department of Defense (DoD)-implementing directives and manuals; Foreign Military Service (FMS) pricing of materiel and services; flow and accounting of funds; the FMS trust fund; obligation and expenditure authority; payment schedules; performance reporting and reimbursement, including the FMS delivery transaction, FMS billing statement (DD Form 645), Defense Finance and Accounting Service Denver and Indianapolis Centers (DFAS) feedback reports, the Defense Integrated Financial System (DIFS); and case reconciliation, and closure. The course is interspersed with studies of the organizations and functions concerned, including the military departments (MILDEPs) and the DFAS, and their interrelationship and involvement. Click on Continuous Learning Points for the SAM-CF course for Acquisition and other Professional Development Program points which can be acquired.

ID: SCM-CF

Prerequisites: N/A

Competencies: Security Program Management

Delivery Type: Instructor-Led

Level: Not Specified

Length: 5 Days

Cost (Type): Not Specified

Provider: DoD Defense Institute of Security Assistance Management

Entry Date: 06/27/2011

Update: 02/16/2012

Link: http://www.disam.dsca.mil/pages/courses/onsite/scm-cf.aspx

T/E26 - PDU 40

Course No Longer Offered

ID: SCM-AT
Prerequisites: N/A
Competencies: Security Tools and Methods
Delivery Type: Instructor-Led

Level: Not Specified
Length: 5 Days
Cost (Type): Not Specified
Provider: DoD Defense Institute of Security Assistance Management

Link: http://www.disam.dsca.mil/pages/courses/onsite/scm-at.aspx

GETTING STARTED SEMINAR FOR NEW FSOS

T/E28 - PDU 12

This course provides new Facility Security Officers (FSOs) the opportunity to apply fundamental National Industrial Security Program (NISP) requirements in a collaborative classroom environment and develop a network of professional associates. Topics discussed are based on material presented in the prerequisite course, FSO Role in the NISP (IS021.06).

ID: IS 121.01

Prerequisites: FSO Role in the NISP (IS021.06)

Competencies: Physical Security, Information Security, Operations Security

Delivery Type: Instructor-Led

Level: Introductory

Length: 1.5 Days

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/27/2011

Update: 03/27/2012

Link: http://www.dss.mil/cdse/catalog/classroom/IS121.html

BUSINESS STRUCTURES IN THE NISP

T/E29 - PDU 2

Enables the student to recognize the business structure of any facility participating in the National Industrial Security Program (NISP) and obtain key information from business records relevant to the facility being cleared in the NISP. The course covers the most common business structures IS Reps encounter when processing a company for a facility clearance.

ID: IS051.16
Prerequisites: None
Competencies: Physical Security
Delivery Type: Web-Based Training

Level: Introductory
Length: 2 Hours
Cost (Type): No
Provider: DoD > DSS > CDSE
Entry Date: 06/27/2011
Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/elearning/IS051.html

FSO ROLE IN THE NISP

T/E30 - PDU 3.5

Describes the role of the Foreign Service Officer (FSO) in the National Industrial Security Program (NISP). The course also identifies resources available to FSOs which enable them to successfully perform in this role.

ID: IS021.06
Prerequisites: None
Competencies: Physical Security
Delivery Type: Web-Based Training

Level: Not Specified
Length: 3.5 hours
Cost (Type): No
Provider: DoD > DSS > CDSE
Entry Date: 06/27/2011
Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/elearning/IS021.html

FSO PROGRAM MANAGEMENT FOR POSSESSING FACILITIES

T/E31 - PDU 43

This program of study prepares individuals for the duties and responsibilities of a Facilities Service Office (FSO) in a contractor facility participating in the National Industrial Security Program (NISP). The FSO Program Management for FSOs at Possessing Facilities (facilities with approved storage for classified material) complies with the training requirements stated in paragraph 3-102 of the National Industrial Security Program Operating Manual (NISPOM) (DoD 5220.22-M).

ID: IS030.CU

Prerequisites: None

Competencies: Security Program Management, Physical Security

Delivery Type: Web-Based Training

Level: Beginner

Length: 42 Hours 45 Minutes

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/27/2011

Update: 03/27/2012

Link: http://www.dss.mil/cdse/catalog/curricula/IS030.html

FSO ORIENTATION FOR NON-POSSESSING FACILITIES

T/E32 - PDU 34.5

This program of study prepares individuals for the duties and responsibilities of a Facility Security Officer (FSO) in a contractor facility participating in the National Industrial Security Program (NISP). The FSO Orientation for FSOs at non-possessing facilities (facilities with no approved storage for classified material) complies with the training requirements stated in paragraph 3-102 of the National Industrial Security Program Operating Manual (NISPOM) (DoD 5220.22-M).

ID: IS020.CU

Prerequisites: None

Competencies: Security Program Management, Physical Security

Delivery Type: Web-Based Training

Level: Introductory

Length: 34 Hours 15 Minutes

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/27/2011

Update: 03/27/2012

Link: http://www.dss.mil/cdse/catalog/curricula/IS020.html

INTRODUCTION TO INDUSTRIAL SECURITY

T/E33 - PDU 1

This course is an interactive Web-based course. The course provides an introduction to the Department of Defense (DoD) Industrial Security Program. The course presents the legal and regulatory basis for the program and how the program is implemented throughout DoD. This course includes an overview of DoD implementation of the National Industrial Security Program (NISP) and discussion of including in contracts security requirements that are outside the scope of NISP.

ID: IS011.16

Prerequisites: None

Competencies: Program Security, Information Security

Delivery Type: Web-Based Training

Level: Introductory

Length: 1 Hour

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/27/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/elearning/IS011.html

SAFEGUARDING CLASSIFIED INFORMATION IN THE NISP

T/E34 - PDU 2.5

This course is an interactive Web-based course covering rules and procedures for protecting classified information and material in the National Industrial Security Program (NISP). Course content is derived primarily from the "National Industrial Security Program Operating Manual (NISPOM)," DoD 5220.22M chapter 5. Lessons cover requirements and procedures for safeguarding classified information including requirements for control and accountability, storage, disclosure, reproduction, and disposition of classified information.

ID: IS109.16

Prerequisites: None

Competencies: Information Security, Classification Management

Delivery Type: Web-Based Training

Level: Introductory

Length: 2.5 Hours

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/27/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/elearning/IS109.html

NISPOM CHAPTER 8 REQUIREMENTS FOR INDUSTRY

T/E35 - PDU 10

The course in its entirety introduces the security requirements for safeguarding classified information being processed and stored in information systems at cleared contractor facilities through an in-depth review of Chapter 8 of the National Industrial Security Program Operating Manual (NISPOM) and is the prerequisite for the NISPOM Chapter 8 Implementation (IS302.01) course. The Introduction and Modules 1-6 can be completed before registering for the final examination but is not required to take the exam.

ID: IS201.16

Prerequisites: None

Competencies: Classification Management

Delivery Type: Web-Based Training

Level: Introductory

Length: 10 Hours

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/27/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/curricula/IS201.html

INFORMATION SECURITY ORIENTATION

T/E36 - PDU 16

Course No Longer Offered

ID: IF101.01

Prerequisites: None

Competencies: Information Security, Classification Management

Delivery Type: Instructor-Led

Level: Introductory

Length: 2 Days

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/27/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/classroom/IF101.html

T/E37 - PDU 45

This mid-level course provides the student with a comprehensive understanding of policies and procedures of the Department of Defense (DoD) Information Security Program. Lessons emphasize security classification, downgrading and declassification, safeguarding (access and dissemination control, accountability, security storage, disposal and destruction, and transmission), violations and compromises, security education, and program oversight. Students can discuss ideas, issues, problems, and possible solutions with key representatives of those executive branch organizations responsible for the Information Security Program. The intent of this course is to provide knowledge and skills for students to effectively implement and/or oversee DoD Information Security Program policies and guidance.

ID: IS201.01

Prerequisites: The Information Security Management Curriculum (IF020.CU)

Competencies: Information Security, Classification Management, Security Program Management

Delivery Type: Instructor-Led

Level: Mid Level
Length: 7 Days
Cost (Type): No
Provider: DoD > DSS > CDSE
Entry Date: 06/27/2011
Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/curricula/IS201.html

INTRODUCTION TO INFORMATION SECURITY

T/E38 - PDU 2

This course is an interactive Web-based course. The course provides an introduction to the Department of Defense (DoD) Information Security Program. The Introduction to Information Security course provides students with a basic understanding of the legal and regulatory basis for the program and how the program is implemented throughout DoD. After completing this course, the student will be familiar with the DoD Information Security Program.

ID: IF011.16

Prerequisites: None

Competencies: Information Security

Delivery Type: Web-Based Training

Level: Introductory

Length: 2 Hours

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/27/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/elearning/IF011.html

MARKING CLASSIFIED INFORMATION

T/E39 - PDU 1

Examines the requirements and methods for marking classified documents and other classified material. Lessons address general marking requirements, marking originally classified information, marking derivatively classified information, marking special types of documents and materials, changes in markings, marking foreign government information, and marking Atomic Energy information.

ID: IF105.16

Prerequisites: None

Competencies: Classification Management

Delivery Type: Web-Based Training

Level: Not Specified

Length: 1 Hour

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 03/27/2012

Link: http://www.dss.mil/cdse/catalog/elearning/IF105.html

DERIVATIVE CLASSIFICATION

T/E40 - PDU 2

Explains how to derivatively classify national security information from a classification management perspective. The course discusses the responsibilities associated with derivatively classifying information; describes the process and methods for derivatively classifying information; identifies authorized sources to use when derivatively classifying information and explains how to apply authorized sources, through derivatively classifying information based on the concepts of "contained in "revealed by," and compilation.

ID: IF103.16

Prerequisites: None

Competencies: Classification Management

Delivery Type: Web-Based Training

Level: Not Specified

Length: 2 Hours

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/elearning/IF103.html

ORIGINAL CLASSIFICATION

T/E41 - PDU 1.5

Provides the policy guidance for, and purpose of, original classification. The course defines original classification and identifies Original Classification Authority requirements and qualifications; reviews the six steps of the original classification decision process; discusses original classification limitations and prohibitions; explains the basis for determining classification levels and duration; and lists the authorized means for providing classification guidance.

ID: IF102.16

Prerequisites: None

Competencies: Classification Management

Delivery Type: Web-Based Training

Level: Not Specified

Length: 1.5 Hours

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/elearning/IF102.html

SECURITY CLASSIFICATION AND GUIDANCE

T/E42 - PDU 2

This course helps provide Original Classification Authorities (OCAs) and derivative classifiers with the requisite knowledge for developing and employing security classification and declassification guidance. This course identifies U.S. Government and DoD policies applicable for developing classification guidance; explains the classification determination process; outlines the process for security classification guides and other types of classification guidance; and describes the process for developing declassification guides.

ID: IF101.16

Prerequisites: None

Competencies: Classification Management

Delivery Type: Web-Based Training

Level: Not Specified

Length: 2 Hours

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/elearning/IF101.html

TRANSMISSION AND TRANSPORTATION FOR DOD

T/E43 - PDU 2

This course examines the requirements and methods for transmitting or transporting classified information and other classified material in accordance with Department of Defense (DoD) Information Security Program (DoD 5200.1-R) requirements. Lessons explain policy, documentation, preparation, dissemination requirements for specific types of information, and authorized transmission and transportation methods.

ID: IF107.16

Prerequisites: None

Competencies: Classification Management

Delivery Type: Web-based Training

Level: Not Specified

Length: 2 Hours

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/elearning/IF107.html

DOD INFORMATION AWARENESS ASSURANCE

T/E44 - PDU 1

This web-based product provides expanded modules and topics to reflect the constant changing world of information assurance as it relates to information technology. The user is introduced to the principles of IA, its evolution, IA-related policies and laws, and critical infrastructure protection (CIP). The training explains the differences between threats and vulnerabilities and provides information regarding the insider threat, social engineering, and peer-to-peer applications. The user is presented with the concept of malicious code, including its impacts and the methods it uses to infect information systems. Important guidelines for ensuring a secure system, defining classification levels for DoD information, to include personally identifiable information (PII), and outlining your role as a user in protecting this information is also provided. The course also introduces the threats associated with identity theft, spyware, phishing, and how you can protect yourself, in addition to providing security tips to practice in your daily routine to increase your home computer security.

ID: DS-IA101.06

Prerequisites: None

Competencies: Information Assurance and Cyber Security

Delivery Type: Web-Based Training

Level: Not Specified

Length: 1 Hour

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 03/27/2012

Link: http://www.dss.mil/cdse/catalog/elearning/DS-IA101.html

INSIDER THREAT

T/E45 - PDU 0.5

One of the most dangerous security threats today is insider threat. This course, presented by the Joint Counterintelligence Training Academy, describes the impact of insider threat to the Department of Defense and shows how to recognize and report it.

ID: JC-CI101.06

Prerequisites: None

Competencies: Counterintelligence

Delivery Type: Instructor-Led

Level: Not Specified

Length: 30 Minutes

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/elearning/JC-CI101.html

PERSONALLY IDENTIFIABLE INFORMATION

T/E46 - PDU 1

Describes what personally identifiable information (PII) is and why it is important to protect PII. This training reviews a Department of Defense (DoD) organization's responsibilities for safeguarding PII and explains individual responsibilities for PII recognition and protection. Major legal, Federal, and DoD requirements for protecting PII are presented to include the Privacy Act of 1974, E-Government Act of 2002, and the Federal Information Security Management Act (FISMA). Federal guidance from the Office of Management and Budget (OMB) publications is discussed. This training includes the DoD Privacy Program and reviews PII protection measures mandated by recent Office of the Secretary of Defense memoranda. Significant requirements are reviewed for handling PII and reporting any theft, loss, or compromise of this information. This training is required for DoD civilians and DoD contractors who work for Defense Security Service (DSS) and have accounts on DSS networks.

ID: DS-IA101.06

Prerequisites: None

Competencies: Information Assurance and Cyber Security

Delivery Type: Web-Based Training

Level: Not Specified

Length: 45 Minutes

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 03/27/2012

Link: http://www.dss.mil/cdse/catalog/elearning/DS-IF101.html

INTERNATIONAL PROGRAMS SECURITY REQUIREMENTS IPSR-OLL

T/E47 - PDU 24

Covers the principles and procedures that facilitate international technology transfer, export controls, and foreign disclosure. Specific lessons discuss the acquisition process for international program security, controlled unclassified and foreign government information, the National Disclosure Policy (NDP), and the International Traffic in Arms Regulations (ITAR). The export approval and license process is covered along with the role of the Defense Security Service. Other topics include the transfer of classified information, visits and assignments of foreign nationals, Multinational Industrial Security Working Group (MISWG) documents, the Committee on Foreign Investment in the United States (CFIUS), and Foreign Ownership, Control or Influence (FOCI).

ID: IN112.06

Prerequisites: None

Competencies: Program Security, Security Program Management

Delivery Type: Instructor-Led

Level: Introductory

Length: 12 Lessons 24 Hours

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/elearning/IN112.html

OPSEC FUNDAMENTALS

T/E48 - PDU 4

Provides a basic working knowledge of operations security (OPSEC) and how it applies to DoD agencies, Components, and contractors. The course focuses on the history of OPSEC and the OPSEC process as described in NSDD-298. Students choose scenarios which allow them to practice OPSEC in different environments.

ID: IO-OP101.16
Prerequisites: None
Competencies: Operations Security
Delivery Type: Web-Based Training

Level: Introductory
Length: 4 Hours
Cost (Type): No
Provider: DoD > DSS > CDSE
Entry Date: 06/28/2011
Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/elearning/IO-OP101.html

DNI ADJUDICATION SEMINAR - ICD 704

T/E49 - PDU 36

Prepare 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.

ID: FT106.01
Prerequisites: None
Competencies: Personnel Security
Delivery Type: Instructor-Led

Level: Not Specified
Length: 4.5 Days
Cost (Type): No
Provider: DoD > DSS > CDSE
Entry Date: 06/28/2011
Update: 03/28/2012

Link: http://www.dss.mil/cdse/catalog/classroom/FT106.html

DOD ADVANCED PERSONNEL SECURITY ADJUDICATION

T/E50 - PDU 36

This course provides in-depth study of adjudication policy guidelines and the basis for and application of due process in unfavorable personnel security determinations. The course emphasizes evaluation and resolution of complex multiple and sensitive issue cases, and the actions as well as agencies and related requirements involved.

ID: PS301.01

Prerequisites: Successful completion of the DoD Personnel Security Adjudications (PS101.01) course and currently performing in an adjudicative or related position for the past 12 months, with at least 6 months of on-the-job experience after successfully completing the DoD Personnel Security Adjudications Course.

Competencies: Personnel Security

Delivery Type: Instructor-Led

Level: Advanced

Length: 4.5 Days

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/classroom/PS301.html

PERSONNEL SECURITY SEMINAR (CUSTOMIZED) - ADJUDICATION

T/E51 - PDU Varies

Meets specific information security training needs of a requesting organization with emphasis on implementation of national adjudicative guidelines. The content, location, and format of this training is determined by the requester.

ID: PS198.01
Prerequisites: None
Competencies: Personnel Security
Delivery Type: Instructor-Led

Level: Varies
Length: Varies
Cost (Type): No
Provider: DoD > DSS > CDSE
Entry Date: 06/28/2011
Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/classroom/PS198.html

PERSONNEL SECURITY SEMINAR-JPAS

T/E52 - PDU Varies

Meets specific personnel security training needs of a requesting organization with a system overview of JPAS subsystem JCAVS. The content, location and/or format (resident, mobile, or video teleconferencing) of this training is determined by the requester.

ID: PS199.01
Prerequisites: N/A
Competencies: Personnel Security
Delivery Type: Instructor-Led

Level: Advanced
Length: Varies
Cost (Type): No
Provider: DoD > DSS > CDSE
Entry Date: 06/28/2011
Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/classroom/PS199.html

E-QIP OVERVIEW

T/E53 - PDU 0.5

Recommend all e-QIP users complete this course. ** This course provides a high-level overview of the purpose, history, and benefits of the e-QIP system. It outlines the various types of investigations, roles, forms, and processes required for using e-QIP. It is primarily aimed at new system users and/or individuals new to Personnel Security. The course includes knowledge checks to ensure knowledge capture and retention.

ID: PS141.06

Prerequisites: None

Competencies: Personnel Security

Delivery Type: Web-Based Training

Level: Introductory

Length: 25 Minutes

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/personnel-security.html

E-QIP ACCESSING AND NAVIGATING E-QIP

T/E54 - PDU 0.5

** Recommend all e-QIP users complete this course. ** This course teaches students how to access, log into, and navigate the e-QIP system. The course includes walkthroughs with knowledge checks and practical exercises that allow students to practice configuring Web browsers and accessing e-QIP.

ID: PS142.06

Prerequisites: None

Competencies: Personnel Security

Delivery Type: Web-Based Training

Level: Introductory

Length: 25 Minutes

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/personnel-security.html

E-QIP SOLUTIONS TO COMMON ISSUES

T/E55 - PDU 0.5

** Recommend all e-QIP users complete this course. ** This lesson focuses on how to respond to common applicant issues. It also instructs the user on various methods for conducting e-QIP case searches. The course includes walkthroughs with knowledge checks and practical exercises. Participants complete tasks in a virtual e-QIP environment and navigate various screens to practice specific procedures.

ID: PS143.06

Prerequisites: e-QIP Overview (PS141.06) Accessing and Navigating e-QIP (PS142.06).

Competencies: Personnel Security

Delivery Type: Web-Based Training

Level: Introductory

Length: 30 Minutes

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/personnel-security.html

E-QIP INITIATING REQUESTS

T/E56 - PDU 0.5

** Recommend e-QIP Initiators complete this course. ** This lesson teaches learners the tasks involved in initiating investigation requests in e-QIP. The course includes walkthroughs with knowledge checks and practical exercises. Learners complete tasks in a virtual e-QIP environment and navigate various screens to practice specific procedures.

ID: PS144.06

Prerequisites: e-QIP Overview (PS141.06); Accessing and Navigating e-QIP (PS142.06); and Solutions to Common Issues (PS143.06).

Competencies: Personnel Security

Delivery Type: Web-Based Training

Level: Intermediate

Length: 40 Minutes

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/personnel-security.html

E-QIP REVIEWING AND APPROVING REQUESTS

T/E57 - PDU 1

** Recommend e-QIP Reviewers and Approvers complete this course. ** This course covers the fundamentals of reviewing and approving e-QIP requests as well as the Reviewer's and Approver's roles and responsibilities in the process. The course includes walkthroughs with knowledge checks and practical exercises. Participants complete tasks in a virtual e-QIP environment and navigate various screens to practice specific procedures.

ID: PS145.06

Prerequisites: e-QIP Overview (PS141.06); Accessing and Navigating e-QIP (PS142.06); Solutions to Common Issues (PS143.06); and Initiating Requests (PS144.06).

Competencies: Personnel Security

Delivery Type: Web-Based Training

Level: Intermediate

Length: 1 Hour

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/personnel-security.html

E-QIP PROGRAM AND BUSINESS MANAGERS

T/E58 - PDU 0.5

** Recommend electronic Questionnaires for Investigations Processing (e-QIP) Program and Business Managers complete this course. ** This lesson focuses on functional features available to Program Managers and Business Managers in e-QIP. The course includes walkthroughs with knowledge checks and practical exercises. Participants complete tasks in a virtual e-QIP environment and navigate various screens to practice specific procedures.

ID: PS146.06

Prerequisites: e-QIP Overview (PS141.06); Accessing and Navigating e- QIP (PS142.06); Solutions to Common Issues (PS143.06); Initiating Requests (PS144.06); and Reviewing and Approving Requests (PS145.06).

Competencies: Personnel Security, Security Program Management

Delivery Type: Web-Based Training

Level: Intermediate

Length: 25 Minutes

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/personnel-security.html

E-QIP MANAGING USER DATA

T/E59 - PDU 0.5

Recommend e-QIP User Administrators complete this course. This lesson focuses on the tasks involved with creating and managing agency user accounts in e-QIP as performed by the User Administrator. The course includes walkthroughs with knowledge checks and practical exercises. Participants complete tasks in a virtual e-QIP environment and navigate various screens to practice specific procedures.

ID: PS147.06

Prerequisites: e-QIP Overview (PS141.06); Accessing and Navigating e-QIP (PS142.06); Solutions to Common Issues (PS143.06); Initiating Requests (PS144.06); Reviewing and Approving Requests (PS145.06); and Program and Business Manager (PS146.06).

Competencies: Personnel Security

Delivery Type: Web-Based Training

Level: Intermediate

Length: 30 Minutes

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/personnel-security.html

E-QIP MANAGING AGENCY DATA

T/E60 - PDU 0.5

Recommend e-QIP Agency Administrators complete this course. This lesson focuses on the tasks involved with establishing an agency's hierarchy and managing groups in e-QIP as performed by the Agency Administrator. The course includes walkthroughs with knowledge checks and practical exercises. Participants complete tasks in a virtual e-QIP environment and navigate various screens to practice specific procedures.

ID: PS148.06

Prerequisites: e-QIP Overview (PS141.06); Accessing and Navigating e-QIP (PS142.06); Solutions to Common Issues (PS143.06); Initiating Requests (PS144.06); Reviewing and Approving Requests (PS145.06); Program and Business Manager (PS146.06; and Managing User Data (PS147.06).

Competencies: Personnel Security

Delivery Type: Web-Based Training

Level: Advanced

Length: Not Specified

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/personnel-security.html

INTRODUCTION TO PERSONNEL SECURITY

T/E61 - PDU 2

This course introduces the management practices and procedures required to administer the DoD Personnel Security Program (PSP) at the military base/ installation level. The course provides an overview of the elements of the PSP to include: designation of sensitive duties; investigative and adjudicative practices; security officer responsibilities under the PSP one-time access requirements; special security program requirements; and due process procedures. The course identifies the types of personnel security investigations (PSIs), the position sensitivity or duties associated, and the agency authorized to conduct PSIs.

ID: PS113.16

Prerequisites: None

Competencies: Personnel Security

Delivery Type: Web-Based Training

Level: Introductory

Length: 2 Hours

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/elearning/PS113.html

JPAS/JAMS VIRTUAL TRAINING FOR SECURITY PROFESSIONALS

T/E62 - PDU 8

This course is an overview of the Joint Personnel Adjudication System (JPAS) and a detailed explanation of its subsystem, the Joint Adjudication Management System (JAMS), which is used extensively by the Department of Defense (DoD) Central Adjudication Facilities (CAFs) to record eligibility determinations and command access decisions. The course includes demonstrations with knowledge checks and practical exercises. Participants complete tasks in a virtual JPAS environment and navigate various windows and practice specific actions to perform desired functions.

ID: PS124.06

Prerequisites: None

Competencies: Personnel Security

Delivery Type: Web-Based Training

Level: Not Specified

Length: Not Specified

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/elearning/PS124.html

INTRODUCTION TO PERSONNEL SECURITY

T/E63 - PDU 7

This course introduces the management practices and procedures required to administer the Department of Defense (DoD) Personnel Security Program (PSP) at the military base/installation level. The course provides an overview of the elements of the PSP to include: designation of sensitive duties; investigative and adjudicative practices; security officer responsibilities under the PSP; one-time access requirements; special security program requirements; and due process procedures. The course identifies the types of personnel security investigations (PSIs), the position sensitivity or duties associated, and the agency authorized to conduct PSIs.
The target audience is DoD civilian, military and contractor personnel who support the DoD PSP. Non-DoD personnel with similar responsibilities are encouraged to register because elements and concepts contained in the course apply to other Federal personnel security programs. This course is specifically designed to address the needs of individuals requiring an overview of the PSP not directly responsible for managing the program.

ID: PS113.16

Prerequisites: None

Competencies: Personnel Security, Security Program Management

Delivery Type: Web-Based Training

Level: Not Specified

Length: 2 Hours

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/elearning/

INTRODUCTION TO PHYSICAL SECURITY

T/E64 - PDU 1

This course is an interactive Web-based course. The course provides an introduction to the Department of Defense (DoD) Physical Security Program. The Introduction to Physical Security course provides students with a basic understanding of the theories and principles involved in the application of physical security in the protection of DoD assets. The course focuses on physical security and the roles people play in the physical security program, introduces the concept of security-in-depth, explores how countermeasures are developed and deployed to deter, delay, detect, or prevent attacks, and physical security planning and implementation.

ID: PY011.06

Prerequisites: None

Competencies: Physical Security

Delivery Type: Web-Based Training

Level: Introductory

Length: 1 Hour

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/elearning/PY011.html

PHYSICAL SECURITY MEASURES

T/E65 - PDU 2.5

This course helps provide the student with a thorough understanding of the physical security measures available for implementation in the protection of Department of Defense (DoD) assets. The course defines the use and purpose of each measure. Topics covered include, but are not limited to, security in depth, intrusion detection systems, fencing, guard forces, and closed circuit television.

ID: PY103.16
Prerequisites: None
Competencies: Physical Security
Delivery Type: Web-Based Training

Level: Not Specified
Length: 2.5 Hours
Cost (Type): No
Provider: DoD > DSS > CDSE
Entry Date: 06/28/2011
Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/elearning/PY103.html

INTRODUCTION TO SPECIAL ACCESS PROGRAMS (SAPS)

T/E66 - PDU 28

This course introduces students to Department of Defense (DoD) Special Access Programs (SAPs). The course describes the SAP environment and discusses the interaction among the executive, legislative, and judicial branches of Government in establishing SAP policy. The roles and responsibilities of oversight and support offices and agencies, and mandatory SAP requirements are reviewed. Lessons address security enhancements across security disciplines, compliance inspection requirements, annual reviews, compliance inspections, and audits.

ID: SA101.01

Prerequisites: Introduction to Information Security (IF011.16/IF011.06) Marking Classified Information (IF105.16/IF105.06) Introduction to Personnel Security Management (PS113.16/PS113.06) Special Access Program (SAP) Overview (SA001.16/SA001.06)

Competencies: Operations Security, Personnel Security, Classification Management

Delivery Type: Web-Based Training

Level: Introductory

Length: 3.5 Days

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/classroom/SA101.html

SAP MID-LEVEL MANAGEMENT

T/E67 - PDU 36

This course offers an in-depth explanation of Special Access Program (SAP) security management. The course focuses on student ability to determine enhanced security requirements based on the threat and vulnerability of SAPs. Students are given scenarios to practice adjusting security countermeasures throughout the SAP life cycle in response to the changing threat. Students review, revise, or write security-related supporting documentation such as treaty, physical security, and transportation plans.

ID: SA201.01

Prerequisites: SAP Orientation/ Introduction to Special Access Programs (SAPs) (SA101.01) Risk Management for DoD Security Programs (GS102.16/ GS102.06)

Competencies: Security Program Management, Vulnerabilities Assessment and Management, Physical Security

Delivery Type: Instructor-Led

Level: Intermediate

Length: 4.5 Days

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/classroom/SA201.html

SAP OVERVIEW

T/E68 - PDU 1.5

This course will provide students with an overview of the Department of Defense (DoD) Special Access Program (SAP) environment, including its history, purpose, life-cycle, approval process, and roles and responsibilities.

ID: SA001.16

Prerequisites: None

Competencies: Information Security, Physical Security, Personnel Security

Delivery Type: Web-Based Training

Level: Introductory

Length: 1.5 Hours

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/elearning/SA001.html

ORIENTATION TO SAP SECURITY COMPLIANCE INSPECTIONS

T/E69 - PDU 16

This course provides students with policy and direction to ensure inspections are standardized, equitable, and consistent across inspection agencies utilizing the Joint Air Force, Army, Navy (JAFAN) manuals. The course reinforces policies and procedures established for the inspection of a Special Access Program (SAP) and its related functional areas as directed by the SAP Central Office (SAPCO) to validate compliance with Government requirements. Students develop the concept of inspection by observing and interacting rather than relying on the inspection checklist.

ID: SA210.01

Prerequisites: Successful completion of the SAP Orientation/Introduction to Special Access Programs (SAPs) (SA101.01).

Competencies: Personnel Security, Information Security

Delivery Type: Instructor-Led

Level: Not Specified

Length: 2 Days

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/classroom/SA210.html

Note: Secret-student clearance eligibility and access information must be documented in the Joint Clearance Access Verification System (JCAVS)

DOD SECURITY SPECIALIST CURRICULUM

T/E70 - PDU 35

This curriculum identifies the prerequisite training requirements for attending the Department of Defense (DoD) Security Specialist Course, GS101.01. This program of study will provide individuals with a comprehensive introduction to the four major security disciplines (Information, Physical, Personnel, and Industrial Security) outlined in the DoD security programs. The intent of this online program of study is to provide the knowledge and skills to prepare individuals to effectively apply their understanding of the DoD security programs during their course of study while attending the instructor-led DoD Security Specialist Course.

ID: GS020.CU

Prerequisites: Security Policies, Principles and Programs (GS140.06) Storage Containers and Facilities (PY105.06) Physical Security Planning and Implementation (PY106.06)

Competencies: Information Security, Physical Security, Personnel Security

Delivery Type: Web-Based Training

Level: Not Specified
Length: 35 Hours
Cost (Type): No
Provider: DoD > DSS > CDSE
Entry Date: 06/28/2011
Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/curricula/GS020.html

RISK MANAGEMENT FOR DOD SECURITY PROGRAMS

T/E71 - PDU 3

Outlines the risk management process that practices application of a systematic approach to acquiring and analyzing information necessary for protecting assets and allocating security resources. The goal of this course is to provide security professionals with an analytical risk management process addressing five steps: Asset Assessment, Threat Assessment, Vulnerability Assessment, Risk Assessment, and Countermeasure Determination.

ID: GS102.16

Prerequisites: None

Competencies: Incident Response, Vulnerabilities Assessment and Management

Delivery Type: Web-Based Training

Level: Not Specified

Length: 3 Hours

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/elearning/GS102.html

SECURITY AWARENESS FOR EDUCATORS (SAFE)

T/E72 - PDU 24

This course discusses how to create an effective security awareness and education program and identifies solutions for overcoming the challenges anyone tasked with security awareness and education duties faces. The course covers how security professionals can create a program with a limited budget, gain management support, motivate coworkers, promote themselves, and prepare and conduct effective security awareness presentations. The course is an interactive blend of presentations, group workshops, and practical exercises during which attendees work in groups tackling challenges and sharing solutions.

ID: GS103.01

Prerequisites: (GS104.16/GS104.06)

Competencies: Security Education and Training, Security Program Management

Delivery Type: Instructor-Led

Level: Advanced

Length: 3 Days

Cost (Type): No

Provider: DoD>DSS>CDSE

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/classroom/GS103.html

DEVELOPING A SECURITY EDUCATION AND TRAINING PROGRAM

T/E73 - PDU 2

This course is an interactive Web-based course. The course provides a thorough understanding of the DoD and National Industrial Security Program (NISP) policy requirements, best practices and instructional methods for developing and implementing a security education and training program. After completing this course, the student will be familiar with the requirements for security education and training program and the knowledge to develop a program at student location.

ID: GS104.16

Prerequisites: None

Competencies: Security Education and Training

Delivery Type: Web-Based Training

Level: Not Specified

Length: 2 Hours

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 06/28/2011

Update: 03/27/2012

Link: http://www.dss.mil/cdse/catalog/elearning/GS104.html

T/E74 - PDU 4.5

The Information Assurance Policy and Technology (IAP&T) training has been created for Information Assurance Officers (IAOs), Information Assurance Managers (IAMs) and System Administrators (SAs) to aid them in successfully performing their duties in accordance with DoD guidance, pertaining to the defense of DoD information and DoD information systems. Individuals whose duties include IA policy and oversight, inspection and audit, or other functions supporting the Information Assurance mission, will find this course useful and meaningful. Depending on your Command, Service, or Agency, the completion of this online course could help the student meet the standards for Level 1 System Administrator certification. This product updates and replaces the IAP&T dated 01/09 version 4.0.

ID: IAP&T

Prerequisites: None

Competencies: Information Assurance/Cyber Security

Delivery Type: Web-Based Training

Level: Advanced

Length: 4.5 Hours

Cost (Type): Not Specified

Provider: DoD> DISA>IA Education, Awareness & Training

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://iase.disa.mil/eta/online-catalog.html

INFORMATION ASSURANCE FOR PROFESSIONALS SHORT

T/E75 - PDU 3

This product contains specific information related to the topics listed below. IA Roles and Responsibilities Short introduces the Information Assurance hierarchy, including the roles and responsibilities of key leadership positions as well as the responsibilities of all Authorized Users. (25 min) Auditing Logs for IA Managers Short introduces the auditing responsibilities of IA Managers. It describes the audit log and event information displayed by the system's auditing software. (20 min) Security Technical Implementation Guides (STIGs) Short introduces the purpose and uses of STIGs. SCADA Short describes how Supervisory Control and Data Acquisition systems function and significant cyber-security issues associated with DoD SCADA systems. (15 min) FISMA Short explains what the FISMA is, why it is important, how it is implemented within the Federal government and the DoD, and identifies where to obtain guidance for FISMA responsibilities. (20 min) IA Vulnerability Management Short describes the vulnerability management process in DoD and the tools that support the process. (20 min) The DoD 8570.01-M IA WIP Short presents an overview of the IA Workforce Improvement Program, defines the DoD IA workforce, and outlines the IA workforce training and certification requirements. (1hr) The Zero Day Attack Short provides an introduction to the steps an IA professional needs to follow if they suspect that their system has been compromised by an attack which otherwise is unknown to the IA technical community (aka Zero Day Attack). (20 min)

ID: Not Specified

Prerequisites: None

Competencies: Information Assurance/ Cyber Security

Delivery Type: Web-Based Training

Level: Introductory

Length: 3 Hours

Cost (Type): Not Specified

Provider: DoD> DISA>IA Education, Awareness & Training

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://iase.disa.mil/eta/online-catalog.html

T/E76 - PDU 1

This product is designed for high-level managers who need to acquire a Computer Network Defense Service Provider (CND SP) for their organization, information assurance (IA) professionals who want to transition into a CND SP career path, and individuals who desire a general knowledge of computer network defense (CND) and CND SPs. This interactive web-based training defines CND, identifies CND requirements for DoD components, key requirements that CND SPs must meet, and the principal services provided by CND SPs. This training presents a high-level explanation of the certification and accreditation (C&A) process for CND SPs. The CND SP principal services are enumerated, to include system protection services, antivirus, system scanning tools, Information Operations Conditions (INFOCON) Program support, Information Assurance Vulnerability Management (IAVM) support, vulnerability assessment monitoring, analysis, and detection services, as well as incident response. An explanation of the training and future certification requirements for those who work as CND SPs is also included.

ID: CND

Prerequisites: None

Competencies: Information Assurance/ Cyber Security, Information Security Vulnerabilities Assessment and Management, Incident Response

Delivery Type: Web-Based Training

Level: Advanced

Length: 1 Hour

Cost (Type): Not Specified

Provider: DoD>DISA>IA Education, Awareness and Training

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://iase.disa.mil/eta/online-catalog.html

ENHANCING INFORMATION ASSURANCE THROUGH PHYSICAL SECURITY

T/E77 - PDU 2

This interactive course is designed for employees needing a general awareness of how the Department's Information Assurance (IA) program is enhanced through physical security. The course consists of four sections. The first section discusses the discipline of physical security, defines terms, and looks at site selection, physical perimeter, and facility controls. The second section describes some of the threats and vulnerabilities involved in protecting the Department's IA, as well as ways to protect the resources. The third section defines the various types of equipment, and addresses what some of the risks are in using them. The last section introduces policy and best practices for protecting the Department's equipment and information.

ID: N/A

Prerequisites: None

Competencies: Information Assurance/ Cyber Security, Information Security Vulnerabilities Assessment and Management, Incident Response

Delivery Type: Web-Based Training

Level: Introductory

Length: 2 Hours

Cost (Type): Not Specified

Provider: DoD>DISA>IA Education, Awareness and Training

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://iase.disa.mil/eta/online-catalog.html

INFORMATION ASSURANCE FOR DOD AUDITORS AND IGS

T/E78 - PDU 8

This interactive web-based training introduces the role of the auditor and inspector in Information Assurance (IA) in the DoD, to include practical challenges concerning the protection of DoD information systems. This training emphasizes the importance of IA to the DoD's mission, key DoD IA operational roles, and Federal Government, as well as DoD, legal and policy guidance for IA. Use of IA and IA-enabled technology in compliance with the International Common Criteria is detailed. Application of mission assurance category (MAC) and confidentiality level for a DoD information system and enclave is explained. The presentation includes an overview of certification and accreditation of information systems in the DoD, with an amplifying discussion of DoD risk management validation. The basic principles of DoD connection approval processes are addressed. The training concludes with a practical exercise using an audit or inspection of a DoD organization at a forward-deployed location to review the knowledge and IA audit techniques presented.

ID: N/A

Prerequisites: None

Competencies: Information Assurance/ Cyber Security, Vulnerabilities Assessment and Management

Delivery Type: Web-Based Training

Level: Not Specified

Length: 8 Hours

Cost (Type): Not Specified

Provider: DoD > DISA > IA Education, Awareness and Training

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://iase.disa.mil/eta/online-catalog.html

WINDOWS SERVER 2003 INCIDENT PREPARATION AND RESPONSE: PART I

T/E79 - PDU 5

This course is intended for Information Assurance (IA) Level II Technicians and Managers and for review by Level III Technicians and Managers. Level I IA Technicians and Managers can use the course to prepare for the network responsibilities of Level II positions. Part I of the course focuses primarily on the Information Assurance mechanisms used in Microsoft® Windows® Server 2003. The course describes file systems, some administrative procedures, server management, and folder and file permissions. Topics on security policy, archiving, logs, host- and network-based intrusion detection, as well as third-party tools are provided. A module on Response presents information about preparation, reaction, notification, recovery options, and working with law enforcement.

ID: IP&R Part I

Prerequisites: None

Competencies: Information Assurance/Cyber Security, Incident Response, Vulnerabilities Assessment and Management

Delivery Type: Web-Based Training

Level: Intermediate/Advanced

Length: 5 Hours

Cost (Type): Not Specified

Provider: DoD>DISA>IA Education, Awareness and Training

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://iase.disa.mil/eta/online-catalog.html

UNIX SECURITY FOR SYSTEM ADMINISTRATION, VER 2.0

T/E80 - PDU 10.5

This course provides an overview of UNIX security basics for Systems Administrators (SAs) and Information Assurance Officers (IAOs). Topics covered include: network terminology, a framework of UNIX security relating to SA duties, security tools and commands, and reporting mechanisms. The course can be used to provide a conceptual UNIX Security foundation supporting Department of Defense Technical and Management Level I Information Assurance Certifications. It is also appropriate as a refresher for Technical and Management Level II. The course is designed to help beginning to intermediate SAs and IAOs understand their roles in keeping their system secure; understand vulnerabilities and threats in terms of their origins, methods, and damage capabilities; and identify, classify, and use system commands and other tools to assist in keeping the system secure. Because of the wide variety of system configurations, variations among local policies, and rapid technological changes, task specifics are not emphasized in this course.

ID: N/A

Prerequisites: None

Competencies: Information Assurance/ Cyber Security, Vulnerabilities Assessment and Management

Delivery Type: Web-Based Training

Level: Introductory

Length: 10.5 Hours

Cost (Type): Not Specified

Provider: DoD>DISA>IA Education, Awareness and Training

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://iase.disa.mil/eta/online-catalog.html

SYSTEM ADMINISTRATOR INCIDENT PREPARATION & RESPONSE FOR UNIX, VER 2.0

T/E81 - PDU 6.5

This product was designed to provide Federal System Administrators (SAs) or Information Assurance Officers (IAOs), who have 3 to 5 years of experience, with a follow-on course that builds on "UNIX Security for System Administrators, Version 2." It is intended to provide training in preparing for, recognizing, and responding to information systems security incidents from a generic law enforcement perspective. The course touches on computer crimes and laws, system preparation, logs and auditing, mechanics and indicators of intrusion, and the architectures of some common but complex attacks. Updates include more and newer tools to assist the SA, as well as information from newer versions of policies and resources. Biometrics, steganography, and other complex techniques are introduced. Intrusion reporting is also discussed. Although some technical aspects of intrusion and malicious code are presented, this is NOT a "hacker's" course. The course supports knowledge needed for Information Assurance Technical and Management Level II, and is appropriate as a refresher at Technical Level III.

ID: SAIPR UNIX

Prerequisites: None

Competencies: Incident Response, Information Assurance/Cyber Security

Delivery Type: Web-Based Training

Level: Intermediate

Length: 6.5 Hours

Cost (Type): Not Specified

Provider: DoD>DISA>IA Education, Awareness and Training

Entry Date: 06/28/2011

Update: 02/16/2012

Link: http://iase.disa.mil/eta/online-catalog.html

CYBERLAW 1 VER. 1.0

T/E82 - PDU 6

CyberLaw I is a web-based training product for DoD lawyers who need to understand the legal and policy issues, both current and emerging, associated with IA and Critical Infrastructure Protection (CIP). DoD lawyers will gain an increased ability to recognize and properly analyze legal issues in Cyberspace. The presentation begins with an introduction to the internet. The second module, "Law in Cyberspace," defines computer crime, discusses the First and Fourth Amendments, and presents statutory considerations to be applied during investigations. This module also discusses the four distinct roles or "lanes of the road" pertinent to Computer Network Defense. References are provided throughout the course for lawyers to follow evolving areas of the law in Cyberspace.

ID: Not Specified

Prerequisites: None

Competencies: Information Assurance/ Cyber Security, Information Security

Delivery Type: Web-Based Training

Level: Not Specified

Length: 6 Hours

Cost (Type): Not Specified

Provider: DoD>DISA>IA Education, Awareness and Training

Entry Date: 06/29/2011

Update: 02/16/2012

Link: http://iase.disa.mil/eta/online-catalog.html

CYBERLAW 2 VER.1.01

T/E83 - PDU 5.5

This product is the second installment in the DoD CyberLaw training suite of products. This course is designed to aid the DoD attorney in keeping abreast of policies and laws that pertain to cybercrime. This course is divided into three sections. The first section discusses issues relating to investigating crime, including the applicability of the Fourth Amendment, honeypots, honeynets, honeygrids, transborder issues, statutory issues, and online undercover operations. The second section addresses issues related to prosecuting crimes and electronic evidence. The third section of this training product addresses post-trial issues and the disposition of evidence.

ID: Not Specified

Prerequisites: CyberLaw 1 ver 1.0

Competencies: Information Assurance/ Cyber Security

Delivery Type: Web-Based Training

Level: Not Specified

Length: 5.5 Hours

Cost (Type): Not Specified

Provider: DoD>DISA>IA Education, Awareness and Training

Entry Date: 06/29/2011

Update: 02/16/2012

Link: http://iase.disa.mil/eta/online-catalog.html

DE-INTRODUCTION TO CYBER INVESTIGATIONS (DE-ICI)

T/E84 - PDU 40

Presents the processes, techniques, specialized documentation, legal guidelines, and requirements for conducting a basic cyber crime investigation through the use of lecture, practical exercises, scenarios and case studies. Please note: This course does not provide the depth needed to conduct an advanced cyber crime investigation (i.e., Intrusions).

ID: RT220

Prerequisites: None

Competencies: Information Assurance/ Cyber Security

Delivery Type: Instructor-Led

Level: Introductory

Length: 40 hours/5 weeks

Cost (Type): No

Provider: DoD> The Defense Cyber Investigations Training Academy

Entry Date: 06/30/2011

Update: 02/16/2012

Link: http://www.dc3.mil/dcita/courseDescriptions/de-ici.php

COMPUTER INCIDENT RESPONDERS COURSE (CIRC)

T/E85 - PDU 45

In this First Response course, students learn how to seize and preserve digital evidence. They get extensive practice imaging hard disks, USB drives, and other media using a variety of methods and tools, including EnCase, FTK Imager, dc3dd, and hardware write-blocking devices. Using several operating systems, students learn to find and extract volatile information of evidentiary value, such as log files, user information, and access rights. They also learn what user information may reside only on network servers, such as user profile and e-mail content, and how to acquire it. Networking sections emphasize network topology so that students understand which log files contain potential evidence and where to find them. In addition, students get extensive practice collecting images in a network environment.

ID: RT120

Prerequisites: TT110 (INCH) or Test out

Competencies: Incident Response, Information Assurance/Cyber Security

Delivery Type: Instructor-Led

Level: Not Specified

Length: 10 days

Cost (Type): No

Provider: DoD> The Defense Cyber Investigations Training Academy

Entry Date: 06/30/2011

Update: 02/16/2012

Link: http://www.dc3.mil/dcita/courseDescriptions/circ.php

INTRODUCTION TO COMPUTER SEARCH AND SEIZURE

T/E86 - PDU 24

The ICSS course introduces students to the commonly used and accepted procedures for recognizing and seizing computer-related evidence. Emphasis is placed on the protection of original digital media, evidentiary chain of custody, and documentation of procedures. The implications of related legal statutes are also discussed. {Mobile}

ID: RT101

Prerequisites: None

Competencies: Information Assurance/ Cyber Security

Delivery Type: Web-Based Training

Level: Not Specified

Length: 3 days

Cost (Type): No

Provider: DoD> The Defense Cyber Investigations Training Academy

Entry Date: 06/30/2011

Update: 02/16/2012

Link: http://www.dc3.mil/dcita/courseDescriptions/icss.php

ANTI-TERRORISM INTELLIGENCE AWARENESS TRAINING PROGRAM

T/E87 - PDU 8

The Anti-Terrorism Intelligence Awareness Training Program (AIATP) is an introductory awareness program designed to provide line officers and first-line supervisors with an overview of terrorism with a focus on both domestic and international activities, a working knowledge of the criminal intelligence process, an overview of the detection and reporting of indicators of terrorist activities and the reporting of suspicious activity. The program includes a regional terrorism update by the FUSION Center from the area the training is held. Please review the training schedule and apply for a program in your area.

ID: AIATP

Prerequisites: This training is open to any full-time law enforcement officer, especially as a first line officer or supervisor.

Competencies: Counterintelligence, Vulnerabilities Assessment and Management

Delivery Type: Instructor-Led

Level: Entry
Length: 1 day
Cost (Type): No
Provider: DHS>FLETC
Entry Date: 06/30/2011
Update: 02/16/2012

Link: http://www.fletc.gov/osl/tuition-free-training-programs/anti-terrorism-intelligence-awareness-training-program-aiatp/

INTELLIGENCE ANALYST TRAINING PROGRAM

T/E88 - PDU 45

The Financial Fraud Institute (FFI) of the Investigative Operations Division (IOD) of the Federal Law Enforcement Training Center (FLETC), Glynco, Georgia, is home to the Intelligence Analyst Training Program (IATP). CTD is responsible for the training of intelligence analysts criminal research specialists, and investigative analysts from Partner Organizations. The program is open to military, State, and local law enforcement intelligence and investigative analysts on a space-available basis.

ID: IATP

Prerequisites: Not Specified

Competencies: Counterintelligence

Delivery Type: Instructor-Led

Level: Advanced

Length: 9.5 days/76 hours

Cost (Type): Not Specified

Provider: DHS>FLETC

Entry Date: 06/30/2011

Update: 02/16/2012

Link: http://www.fletc.gov/training/programs/investigative-operations-division/economic-financial/intelligence-analyst-training-program-iatp/

INTELLIGENCE AWARENESS FOR LAW ENFORCEMENT EXECUTIVES TRAINING PROGRAM

T/E89 - PDU 8

The Intelligence Awareness for Law Enforcement Executives Training Program (IALEETP) is a 6-hour specialized training program designed to provide State, local, tribal, and campus law enforcement executives with a working knowledge of the National Criminal Intelligence Sharing Plan (NCISP), the criminal intelligence process and their important role in working towards the systematic sharing of information among the law enforcement community. Highlights of the program include an introduction to the National Criminal Intelligence Sharing Plan, the concept of Intelligence Led Policing, and the legal and privacy considerations associated with information collection, storage, and dissemination. The program includes a regional terrorism update by the FUSION Center from the area the training is held. Please review the training schedule and apply for a program in your area.

ID: IALEETP

Prerequisites: State, local, tribal, and campus law enforcement executives (Chiefs, Sheriffs, and other command level personnel). Open to U.S. Citizens ONLY.

Competencies: Security Program Management

Delivery Type: Instructor-Led

Level: Advanced

Length: 1 day

Cost (Type): No

Provider: DHS>FLETC

Entry Date: 06/30/2011

Update: 02/16/2012

Link: http://www.fletc.gov/osl/tuition-free-training-programs

INTRODUCTORY INTELLIGENCE ANALYST TRAINING PROGRAM

T/E90 - PDU 40

This is a 40-hour entry-level computer based program, which provides a historical, legal, and ethical basis for law enforcement intelligence collection, retention, and dissemination. Students are required to complete an intelligence collection project involving a criminal organization. As the class progresses, students prepare various intelligence products such as: a criminal predicate statement; a mission statement; a hypothesis; and, a collection/dissemination plan. Students also utilize Internet research techniques, computer graphics, electronic spreadsheets, and report writing training to analyze and professionally document the results of the intelligence collection project. Course material is presented by subject matter experts in an adult-centered learning environment. Additionally, students must achieve a passing score on a comprehensive written examination, complete an individual collection project, and participate in a group oral presentation to class members and instructors.

ID: IIATP

Prerequisites: State, local, tribal, and campus law enforcement intelligence personnel (Federal and military personnel may attend on a space-available basis). Open to U.S. Citizens ONLY.

Competencies: Counterintelligence

Delivery Type: Instructor-Led

Link: http://www.fletc.gov/osl/

Level: Introductory
Length: 5 days
Cost (Type): No
Provider: DHS>AFOIS>FLETC
Entry Date: 07/05/2011
Update: 02/16/2012

INTERNET INVESTIGATIONS TRAINING PROGRAM

T/E91 - PDU 40

After providing a foundation of how the Internet functions and the technology related to it, the Internet Investigations Training Program (IITP) will focus on two different aspects of Internet investigations. First, the program will address the investigation of crimes that use the Internet to conduct or facilitate the crime and, secondly, will also focus on live online investigations on the Internet. The types of investigations discussed will include child pornography, child predators, identity theft, money laundering, financial and fraud, as well as a general discussion of cybercrime in general. The use of social networking and Internet gaming sites for criminal activity will also be discussed. Other topics will include tracking emails and undercover operations on the Internet. Students will be taught how to protect their identities and personal information on the Internet, and how to set up an investigative computer.

ID: IITP

Prerequisites: The target audience will be Criminal Investigators, Non-Criminal Investigators, Criminal Analysts, Intelligence Analysts, and Intelligence Specialists from the Federal, State, and local law enforcement community who are tasked with conducting cybercrime investigations. Students should possess a working knowledge of computers, computer-related programs and the Internet.

Competencies: Information Assurance/Cyber Security

Delivery Type: Instructor-Led

Level: Advanced
Length: 10 Days
Cost (Type): No
Provider: DHS>FLETC
Entry Date: 05/05/2011
Update: 02/16/2012

Link: http://www.fletc.gov/training/programs/investigative-operations-division/economic-financial/internet-investigations-training-program-iitp/

LAW ENFORCEMENT MANAGER TRAINING PROGRAM

T/E92 - PDU 45

The Law Enforcement Manager Training Program (LEMTP) is a middle management training program designed to provide law enforcement second-line supervisors and seasoned managers with the skills and competencies needed to be successful. The LEMTP provides law enforcement professionals the opportunity to learn and network with peers who share similar experiences, problems, challenges and other concerns that law enforcement is facing today and will face in the future. It focuses on competencies that are tied directly to personal and organizational skills of the second-line supervisor.

ID: LEMTP

Prerequisites: This program is not intended for entry-level supervisors. It is designed for Federal law enforcement managers who have completed a first-line supervisory training program such as the Law Enforcement Supervisor Leadership Training Program (LESLTP) or one who has served in an operational supervisory role.

Competencies: Security Program Management

Delivery Type: Web-Based Training

Level: Mid-Level
Length: 5 days
Cost (Type): Not Specified
Provider: DHS>AFOIS>FLETC
Entry Date: 07/05/2011
Update: 02/16/2012

Link: http://www.fletc.gov/training/programs/leadership-and-international-capacity-building-division/law-enforcement-manager-training-program-lemtp

LEADERSHIP THROUGH UNDERSTANDING HUMAN BEHAVIOR TRAINING PROGRAM

T/E93 - PDU 24

To provide law enforcement leaders with a training vehicle that can help them develop more effective workgroups and teams. Workgroup and team members develop a better understanding of themselves, interpersonal dynamics, and how their strengths, weaknesses, and roles within workgroups and teams affect mission outcomes. Participants learn how to adapt and capitalize on each other's strengths in order to have more effective mission outcomes. The program is designed to be customized based on specific needs of the customer. Emotional intelligence and "people skills" are competencies needed in every employee. Organizations that recognize the importance of developing their people in these areas benefit by having more productive working relationships, better outcomes, communications, less conflict, and enhanced personal satisfaction in their workgroups and teams. The first step in this journey is for team members to understand themselves. The program starts by developing emotional self-awareness and the ability to recognize and modify, if needed, one's own communications or behavioral style in order to build relationships. As workgroups/members start to develop an understanding of each other's behavioral strengths and value systems, collectively they start to develop strategies to synergize the work product to effectively accomplish goals. Leadership can look into ways that members work together, both as a group and at the level of individual relationships. This information can be used to establish more effective workgroups and teams by capitalizing on the strengths each individual brings to the group. In more specific terms, this training can yield valuable information on particular aspects of the team development process. This conceptual understanding is essentially a starting point for developing more effective workgroups and teams within your organization.

ID: LTUHB

Prerequisites: This program is designed as a career development tool; thus, who may attend is determined by participating agency needs.

Competencies: Security Program Management

Delivery Type: Instructor-Led

Level: Multiple Levels
Length: 3 days
Cost (Type): Not Specified
Provider: DHS>AFOSI
Entry Date: 07/05/2011
Update: 02/16/2012

Link: http://www.fletc.gov/training/programs/leadership-and-international-capacity-building-division/leadership-through-understanding-human-behavior-training-program-ltuhbtp/

LAW ENFORCEMENT SUPERVISOR LEADERSHIP TRAINING PROGRAM

T/E94 - PDU 45

This program is a career development tool that provides a unique opportunity for law enforcement professionals to develop and refine their leadership skills in a leadership/supervisory training program designed for law enforcement. The instructors in this program are all current or former supervisory law enforcement professionals. These professionals bring the unique understanding of the law enforcement culture, and the practical knowledge of how to meet the challenges that law enforcement leaders will face in operational law enforcement settings. Participants in this program will gain an understanding of how to apply basic leadership knowledge, skills, and abilities (KSAs) in order to obtain the highest level of performance and accountability. This program focuses the new law enforcement leader's skill base in the three key enablers of human capital leadership: people, process, and technology. The program focuses heavily on the most important enabler of human capital leadership — "people." This leadership development journey first starts with a self-assessment, and the understanding that people are assets whose value can be enhanced through investment and understanding. The law enforcement leadership journey continues by understanding and aligning their organization's "shared vision" with mission, vision for the future, core values, goals and objectives, and, most important, leading by example. The KSA topical areas include leadership skills through understanding and adapting to human behaviors, communication skills, team building, conflict management, human resource management, legal responsibilities, stress management, workplace diversity, performance skills, briefing skills, and situational decision-making skills. Taking into consideration life and work experience, participants will explore these topics and develop skills by means of an adult learning model that employs lecture, practical exercises, case studies and self-directed learning. This program addresses the competencies needed to be effective as a leader in the law enforcement community. The courses in this program focus heavily on the human capital development disciplines and the law enforcement mission and culture. To accomplish this, LELI has partnered with some of the best-known experts on leadership from the private sector. This enables LELI to deliver some of the best courses on leadership to our customers. These programs and courses have been customized to address concerns and needs of the law enforcement community. This partnership has proven to be an investment that continues to help develop the next generation of law enforcement leadership for this nation.

ID: LESLTP

Prerequisites: This program is designed as a career development tool; thus, who may attend is determined by participating agency needs.

Competencies: Security Program Management

Delivery Type: Instructor-Led

Level: Multiple

Length: 8 days

Cost (Type): Not Specified

Provider: DHS>AFOSI>FLETC

Entry Date: 07/05/2011

Update: 02/16/2012

Link: http://www.fletc.gov/training/programs/leadership-and-international-capacity-building-division/law-enforcement-supervisor-leadership-training-program-lesltp/

SITUATIONAL LEADERSHIP II FOR LAW ENFORCEMENT TRAINING PROGRAM

T/E95 - PDU 24

The role of the law enforcement supervisor and manager has changed. In the past, supervisors and managers were expected to be the boss, evaluator, judge, and critic. In today's rapidly changing world the authoritarian manager that valued compliance, conformity, and command control hierarchies will not be able to keep up with the pace of change. Today, the law enforcement manager and supervisor must become a partner, facilitator, cheerleader, supporter, and coach in order to be successful. As law enforcement leaders, our task is to accomplish the organizational mission by means of our greatest resource, our people. As law enforcement leaders, we must understand that the value of diversity is that each individual brings his or her unique experience, skills and commitment to the organization and its mission. Today's law enforcement leader must be able to successfully use a variety of leadership styles depending on the task, mission, and individual. Situational Leadership® II can provide you with a variety of leadership tools that can enhance your effectiveness and success as a supervisor, in this rapidly changing world. This program teaches the leadership model developed and perfected by Dr. Ken Blanchard, and his colleagues at The Ken Blanchard Companies. The FLETC Law Enforcement Leadership Institute (LELI) and The Ken Blanchard Companies have collaborated to customize the program for law enforcement leaders and managers. It provides a unique opportunity for law enforcement professionals to not only refine their supervisory and leadership skills, but more importantly, to use Situational Leadership (SL)® II to develop their people. The instructors are current or former law enforcement professionals and have been qualified by The Ken Blanchard Companies to present the program. These professionals bring a unique understanding of the law enforcement culture, and practical knowledge of how to meet the challenges that face a law enforcement supervisor in operational settings. Participants in this program will gain an understanding of how to apply SL® II in both their personal lives and their law enforcement careers. Participants will explore topics to develop skills using an adult learning model that employs lecture, case studies, practical exercises, and self-directed learning. This program is highly participatory and hands-on.

ID: SLTP

Prerequisites: This program is designed as a career development tool; thus, who may attend is determined by participating agency needs.

Competencies: Security Program Management

Delivery Type: Instructor-Led

Level: Multiple
Length: 3 days
Cost (Type): Yes
Provider: DHS>AFOSI>FLETC
Entry Date: 07/05/2011
Update: 02/16/2012

Link: http://www.fletc.gov/training/programs/leadership-and-international-capacity-building-division/situational-leadership-aeii-for-law-enforcement-training-program-sliitp/

INTELLIGENCE ANALYSIS SUMMER PROGRAM (UNDERGRADUATE)

T/E96 - PDU 45

NSA's Intelligence Analysis Program offers rising college seniors the opportunity to receive training in a multi-faceted cryptologic discipline that involves research, analysis, and the presentation of findings that enable us to provide the fullest possible Signals Intelligence picture to U.S. policymakers, military commanders, and other Intelligence Community members. NSA's Intelligence Analysis Summer Program is an intensive 12-week program for undergraduates entering the final year of an undergraduate degree program (juniors at the time of application). Participants receive training in multiple cryptologic disciplines, including technical research and topical analysis. They research current foreign intelligence issues and present the results of their analysis. Their findings become part of NSA's effort to provide the fullest possible Signals Intelligence (SIGINT) picture to U.S. policymakers, military commanders, and other Intelligence Community members. The program consists of formal classroom instruction, workshops, and agency facilities tours. Participants gain practical and theoretical knowledge of NSA, the SIGINT process, and the U.S. Intelligence Community. Classroom training is combined with mentoring by experienced NSA analysts to increase our insight into high-priority intelligence targets. Participants receive training in current analytic tools and tradecraft, conduct extensive independent research using numerous databases, prepare findings in a variety of formats, and deliver a final project report to the sponsoring analytic organization.

ID: Not Specified

Prerequisites: Required: U.S. citizenship

Required: Eligible to be granted a security clearance

Required: Full time undergraduate student entering the final year of an undergraduate degree program (juniors at the time of application)

Required: Applicant must be available for the entire length of the program.

Competencies: Information Security, Vulnerabilities Assessment and Management

Delivery Type: Instructor-Led

Level: Undergraduate

Length: 12 weeks

Cost (Type): Not Specified

Provider: National Cryptological School

Entry Date: 07/05/2011

Update: 02/16/2012

Link: http://www.nsa.gov/careers/opportunities_4_u/students/undergraduate/iasp.shtml

SUMMER INTERN PROGRAM FOR INFORMATION ASSURANCE

T/E97 - PDU 45

The Summer Intern Program for Information Assurance (SIP/IA) is a full-time, 12-week program open to select college upperclassman and graduate students who are concentrating their studies in the disciplines of information assurance. To participate in this program, the student must return to school for at least one semester following the internship.

For purposes of this program, IA encompasses the scientific, technical, and management disciplines required to ensure computer and network security, such as:

* System/network administration and operations
* Systems security engineering
* Information assurance systems and product acquisition
* Cryptography
* Threat and vulnerability assessment, including risk management
* Cyber security
* The operations of computer emergency response teams
* Information assurance training, education and management
* Computer forensics
* Defensive information operations

ID: (SIP/IA)

Prerequisites: Must be a U.S. citizen. Must be eligible to be granted a security clearance. A GPA of 3.0 or higher is preferred. Must be a college junior or a student pursuing graduate school.

Competencies: Information Assurance/ Cyber Security

Delivery Type: Instructor-Led

Level: Undergraduate

Length: 12 weeks

Cost (Type): Yes

Provider: National Cryptological School

Entry Date: 07/05/2011

Update: 02/16/2012

Link: http://www.nsa.gov/careers/opportunities_4_u/students/undergraduate/sip.shtml

OPSEC OVERVIEW

T/E98 - PDU 1

eLearning course. No pre-registration is required; National Training Center (NTC) learners may launch and take the course at any time. Completions will be automatically logged to the Learner's Learning History. Please note: This eLearning course replaces ISC-141DW OPSEC Overview web-based course, previously available from the NTC Website. These materials can be used for initial OPSEC orientations, periodic OPSEC refresher training, and general security education or motivational purposes.

ID: ISC-141DE

Prerequisites: None

Competencies: Operations Security

Delivery Type: Web-Based Training

Level: Not Specified

Length: 1 hour

Cost (Type): Not Specified

Provider: DOE>National Training Center

Entry Date: 07/05/2011

Update: 02/16/2012

Link: http://ntc.doe.gov/shared/courses.aspx

LEGAL ASPECT OF INQUIRIES

T/E99 - PDU 16

This correspondence course is available as a .pdf download in the Online Learning Center (OLC2). Please download, print, and complete course per instructions. No registration is required. This unclassified, introductory-level, self-paced correspondence course, with accompanying online video instruction, provides an understanding of the legal issues associated with inquiries into incidents of security concern. The course's purpose is to assist in the conduct of inquiries that protect DOE security interests, without violating the 4th or 5th amendment legal rights of DOE or DOE-contractor employees. Included are review questions for which the minimum passing score is 80%.

AUDIENCE: DOE and DOE-contractor personnel who are or will be responsible for conducting inquiries into incidents of security concern.

ID: ISC-202DV

Prerequisites: None

Competencies: Security Program Management

Delivery Type: Other

Level: Not Specified

Length: 16 hours

Cost (Type): Not Specified

Provider: DOE>National Training Center

Entry Date: 07/05/2011

Update: 02/16/2012

Link: http://ntc.doe.gov/shared/courses.aspx

SPECIAL PROGRAM SECURITY OFFICER (SPSO)

T/E100 - PDU 24

The course prepares participants to function as Special Program Security Officers (SPSOs) for special access programs (SAPs). REQUIRED: There is read-ahead material that all registered students will receive about 4 weeks prior to the class. Students are required to read this material before the first day of the class.

RECOMMENDED: It is also recommended that students take the following National Training Center (NTC) classroom courses, either before or after taking ISC-222, to enhance their education as an SPSO: ISC-121DE Introduction to Classified Matter Protection and Control (CMPC); ISC-221 Classified Matter Protection and Control I; ISC-301 Conduct of Inquiries; PHY-128DB Introduction to Basic Survey; PHY-130 Basic Survey; PHY-210DB Facility Security Officer Orientation.

ID: ISC-222

Prerequisites: None

Competencies: Information Security, Classification Management

Delivery Type: Instructor-Led

Level: Not Specified

Length: 24

Cost (Type): Yes

Provider: DOE>National Training Center

Entry Date: 07/05/2011

Update: 02/16/2012

Link: http://ntc.doe.gov/shared/courses.aspx

TECHNICAL SURVEILLANCE COUNTERMEASURES

T/E101 - PDU 24

This course provides generic information for individuals associated with the DOE Technical Surveillance Countermeasures (TSCM) Program. The course serves as a general overview of the TSCM Program, touching on various levels of responsibilities for those who are involved in either DOE or national-level programs. It does not provide site-specific instructions, but rather, it points out the basic requirements to the students and shows the inter-relationship between TSCM and other security programs. It also covers threat analysis and demonstrates selected TSCM equipment.

REQUIRED: Clearance for access to Secret National Security Information.

ID: ISC-234

Prerequisites: None

Competencies: Security Program Management

Delivery Type: Instructor-Led

Level: Not Specified

Length: 16 hours

Cost (Type): Not Specified

Provider: DOE>National Training Center

Entry Date: 07/05/2011

Update: 02/16/2012

Link: http://ntc.doe.gov/shared/courses.aspx

OPERATIONS SECURITY OPSEC

T/E102- PDU 24

This course focuses on resources, policies, and training that deny unauthorized individuals or groups access to classified and sensitive-unclassified information. Emphasis is placed on the exploitable sources of information normally available to an adversary and on cost-effective countermeasures to deny or delay the availability of such information. The course requires a minimum score of 80% based on administered testing results and completion of a 10-hour practical exercise.

ID: ISC-241

Prerequisites: None

Competencies: Operations Security

Delivery Type: Instructor-Led

Level: Not Specified

Length: 24 hours

Cost (Type): Not Specified

Provider: DOE>National Training Center

Entry Date: 07/05/2011

Update: 03/28/2012

Link: http://ntc.doe.gov/shared/courses.aspx

CONDUCT OF INQUIRIES

T/E103 - PDU 24

This course will address policies, procedures, and reporting requirements for inquiries into incidents of security concern, to include a review of the legal aspects of conducting an inquiry. It will also cover interview techniques, data-gathering ideas, to include potential contacts, and report writing.

RECOMMENDATIONS: DOE Safeguards and Security information Management System (SSIMS) training, offered through HS-81, Office of Security Assistance.

AUDIENCE: DOE and DOE-contractor personnel who have or will have responsibility for conducting inquiries into incidents of security concern.

ID: ISC-301

Prerequisites: ISC-202DV

Competencies: Information Security, Classification Management, Operations Security

Delivery Type: Instructor-Led

Level: Not Specified

Length: 24 hours

Cost (Type): Not Specified

Provider: DOE>National Training Center

Entry Date: 07/05/2011

Update: 02/16/2012

Link: http://ntc.doe.gov/shared/courses.aspx

SENIOR CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC)

T/E104 - PDU 16

This unclassified, advanced course prepares attendees to perform the following program management tasks: prepare and implement site procedures and various types of security plans; integrate with other safeguards and security functional areas; develop CMPC training/briefings for local needs; prepare for and perform, assist, or oversee various types of CMPC assessments; and develop, as well as process, a deviation request.

AUDIENCE: DOE and DOE-contractor personnel who are assigned CMPC point of contact (POC) duties and responsibilities for implementing and coordinating CMPC functions.

ID: Not Specified

Prerequisites: ISC-121DE (Introduction to Classified Matter Protection and Control (CMPC)) ISC-221

Competencies: Classification Management, Information Security, Security Program Management

Delivery Type: Instructor-Led

Link: http://ntc.doe.gov/shared/courses.aspx

Level: Not Specified

Length: 16 hours

Cost (Type): Not Specified

Provider: DOE>National Training Center

Entry Date: 07/05/2011

Update: 03/28/2012

FOREIGN VISITS AND ASSIGNMENTS HOST TRAINING

T/E105 - PDU 1.5

NEW FORMAT: FIT-130DE has been redeveloped in a new format and is now available on the Online Learning Center (OLC2). This eLearning course focuses on the responsibilities and requirements for hosting foreign nationals under DOE's Unclassified Foreign Visits and Assignments (FV&A) Program. The training is designed to provide timely information using a delivery method that can be accessed on demand and completed within a short timeframe. Topics are divided into the major areas of host activities and responsibilities in the following phases: Prior to the visit/assignment, during the visit/assignment, and after the visit/assignment. Three lessons are included, with each lesson followed by interactive review questions and the National Training Center (NTC) Student Feedback Form. Links to downloadable forms, job aids, and additional resources are provided. Please note that this course is to be used as a training resource only. Completion of the course does not qualify or certify you as an FV&A host; your site has its own requirements for FV&A hosts that you must also fulfill. Please consult your site Unclassified FV&A coordinator for further information on host qualifications

ID: FIT-120DE

Prerequisites: None

Competencies: Program Security

Delivery Type: Web-Based Training

Level: Not Specified

Length: 1.5 hours

Cost (Type): Not Specified

Provider: DOE>National Training Center

Entry Date: 07/05/2011

Update: 02/16/2012

Link: http://ntc.doe.gov/shared/courses.aspx

INTRODUCTION TO DOE PERSONNEL SECURITY

T/E106 - PDU 3

This eLearning course provides a broad overview of the DOE Personnel Security Program. Topics include a program history; the roles and responsibilities of a personnel security program specialist/analyst; an introduction to applicable criteria and procedures as specified in Title 10, Code of Federal Regulations, Part 710 (10 CFR 710); and an overview of the DOE Administrative Review process.

NOTE: This eLearning course replaces PER-100DB correspondence course, previously available as a pdf download on the NTC's LMS.

NOTE: It is not necessary to contact the National Training Center (NTC) Registration Department to take this course. A completion will be automatically added to your transcript. In order to provide proof of completion, students may print a copy of their certificate from the transcript.

ID: PER-100DE

Prerequisites: None

Competencies: Personnel Security

Delivery Type: Web-Based Training

Level: Not Specified

Length: 3 hours

Cost (Type): Not Specified

Provider: DOE>National Training Center

Entry Date: 07/05/2011

Update: 03/28/2012

Link: http://ntc.doe.gov/shared/courses.aspx

PERSONNEL SECURITY SPECIALIST ADJUDICATION TRAINING

T/E107 - PDU 40

This intermediate-level course provides the basic foundation for knowledge and skill training in the DOE security clearance process. Attendees will receive training in the overall DOE Personnel Security Program as it relates to DOE Manual 470.4-5, Personnel Security, and Title 10 Code of Federal Regulations, Part 710 (10 CFR 710), Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material. Students will learn to analyze a case and evaluate factors that lead to an adjudicative decision on individual eligibility for DOE security clearance.

REQUIREMENT: Current performance of duties as a Federal employee or contractor in the DOE Personnel Security Program.

ID: PER-101

Prerequisites: PER-100DE (Introduction to DOE Personnel Security)

Competencies: Personnel Security

Delivery Type: Instructor-Led

Level: Intermediate

Length: 40 hours

Cost (Type): Not Specified

Provider: DOE>National Training Center

Entry Date: 07/05/2011

Update: 03/28/2012

Link: http://ntc.doe.gov/shared/courses.aspx

PERSONNEL SECURITY ANNUAL REFRESHER TRAINING (FY-2011)

T/E108 - PDU 2.5

This eLearning course satisfies, in part, professional education requirements for Personnel Security Specialists within the Department and serves as an annual mandatory training to update and refresh personnel on policies and procedures. The course is written at a level that assumes Personnel Security Specialists have taken and are familiar with the content of the following four courses:

PER-100DE Introduction to DOE Personnel Security; PER-101 Personnel Security Specialist Adjudication Training; PER-203 Interviewing and Advanced Adjudication; PER-300 Administrative Review Hearing Procedures. Topics include a review of Personnel Security basics and the Bond Amendment, analyzing issues of reciprocity, and analyzing issues of finances.

NOTE: Students do not need to contact the National Training Center Registration Department to take this course. A completion will be automatically added to your Learning History. In order to provide proof of completion, students may print a copy of their certificate from the Learning History.

ID: PER-310DE

Prerequisites: None

Competencies: Personnel Security

Delivery Type: Web-Based Training

Level: Not Specified

Length: 2.5 hours

Cost (Type): Not Specified

Provider: DOE>National Training Center

Entry Date: 07/05/2011

Update: 03/28/2012

Link: http://ntc.doe.gov/shared/courses.aspx

PERSONNEL SECURITY AWARENESS BRIEFING FOR KEY OFFICIALS

T/E109 - PDU 1

This beginner-level briefing provides an overview of the roles and responsibilities of the DOE Personnel Security Program, and was developed for all key officials involved in the personnel security process.

ID: PER-099DE

Prerequisites: None

Competencies: Personnel Security, Security Program Management

Delivery Type: Web-Based Training

Level: Beginner

Length: .5 hours

Cost (Type): Not Specified

Provider: DOE>National Training Center

Entry Date: 07/05/2011

Update: 03/28/2012

Link: http://ntc.doe.gov/shared/courses.aspx

INTRODUCTION TO PHYSICAL PROTECTION SYSTEMS

T/E110 - PDU 36

This correspondence course is available as a pdf download in the Online Learning Center (OLC2). Please launch the course contents, download, print, and complete course per instructions. This introductory correspondence course covers all aspects of physical security systems, including threat definition, target identification, detection (exterior and interior sensors, alarm assessment, communications, and display), entry control, and response from forces as well as communications. Also covered are the roles of hardware and technology as they integrate with the roles of protective forces and procedures. (Because the course focuses on physical protection of nuclear materials at fixed sites, it does NOT address protection of materials while they are in transit from site to site.) Included are excerpts from the student notebook, DOE M 470.4-2A Physical Protection Program Manual, DOE M 470.4-3A Protective Force, and the Inspector General Physical Security Systems report. Lessons are reviewed by self-directed quizzes. Student must pass with 80% or better.

REQUIREMENT: A basic understanding of safeguards and security terminology.

ID: PHY-100DB

Prerequisites: None

Competencies: Physical Security, Information Security Management

Delivery Type: Web-Based Training

Level: Not Specified

Length: 36 hours

Cost (Type): Not Specified

Provider: DOE>National Training Center

Entry Date: 07/05/2011

Update: 02/16/2012

Link: http://ntc.doe.gov/shared/courses.aspx

INTERMEDIATE PHYSICAL SECURITY SYSTEMS

T/E111 - PDU 40

This course addresses the following topical areas: current sensor technology, performance-testing procedures, and maintenance to ensure operational performance. DOE M 470.4-2A Physical Protection Program Manual is covered in depth; DOE 0 470.4A Safeguards and Security Program Order and DOE M 470.4.1 Chg 1 Safeguards and Security Program Planning and Management Manual are only covered as they relate to Physical Security Systems. The course is participative, allowing attendees to gain hands-on experience with various physical security systems. Included is a visit to Sandia National Laboratories' Sensor System Test Bed, enabling attendees to see the types and methodologies of tests conducted for DOE. The course includes quizzes and practical exercises.

AUDIENCE: DOE and DOE-contractor personnel responsible for designing, installing, implementing, or evaluating Physical Protection Systems within the DOE. Course emphasis will be on implementation and evaluation.

REQUIREMENTS: Attendees must also have a basic understanding of electronic engineering concepts as they relate to sensor operation and operational experience at their sites (preferably 1-2 years). Attendees should bring walking shoes and jackets, sun block, and a hat. An outside tour will be conducted.

ID: PHY-120

Prerequisites: PHY-100DB

Competencies: Physical Security, Operations Security

Delivery Type: Instructor-Led

Level: Intermediate

Length: 40 hours

Cost (Type): Not Specified

Provider: DOE>National Training Center

Entry Date: 07/05/2011

Update: 02/16/2012

Link: http://ntc.doe.gov/shared/courses.aspx

FACILITY SECURITY OFFICER ORIENTATION

T/E112 - PDU 24

This correspondence course is available as a pdf download in the National Training Center's (NTC) Learning Management System (LMS). Please download, print, and complete course per instructions. No registration is required. This introductory correspondence course provides an overview of the roles and responsibilities of the DOE or DOE-contractor facility security officer. The course emphasizes facility clearance requirements, personnel security, information security, incident reporting, and other related programs. The course references the NISPOM and a comprehensive listing of DOE orders, manuals, guides, forms, and notices. Successful completion of this course is measured by means of the six sets of end-of-lesson written test questions. Successful completion depends upon a minimum score of 80% on each end-of-lesson test. All documents related to this course can be found in their most current state at the following website:
http://www.directives.doe.gov

ID: PHY-210DB

Prerequisites: None

Competencies: Physical Security

Delivery Type: Web-Based Training

Level: Not Specified

Length: 24 hours

Cost (Type): Not Specified

Provider: DOE>National Training Center

Entry Date: 07/05/2011

Update: 02/16/2012

Link: http://ntc.doe.gov/shared/courses.aspx

BASIC SECURITY POLICE OFFICER TRAINING

T/E113 - PDU 45

This is the introductory course for new Security Police Officers (SPOs) entering the DOE protective force community. Using scenario-based training methods, it addresses the knowledge and skills necessary to perform the duties of an SPO. Topics covered include DOE-specific policies and procedures, legal requirements of the SPO and use of intermediate force, firearms training, post and patrol operations, and tactical operations.

MEDICAL RELEASE: Site medical clearance forms MUST be on file with the National Training Center (NTC) prior to attendance. DOE personnel must meet fitness standards as mandated in 10 CFR 1046.

MANDATORY EQUIPMENT: Students must bring seasonal uniforms and outdoor gear plus duty equipment to include: protective mask and filter with carrying pouch, tactical flashlight, handcuffs, Nomex gloves, elbow and knee pads, billed cap or hat, boots that provide ankle support, groin protection and seasonally-appropriate physical training gear. Mat/wrestling-type shoes are recommended.

NOTE: Dependent upon class size, some training days may run longer than stated in course schedule.

ID: PFT-215

Prerequisites: TRF-100D Introduction to Protective Force

Competencies: Not Specified

Delivery Type: Instructor-Led

Level: Beginner

Length: 360 hours

Cost (Type): Not Specified

Provider: DOE>National Training Center

Entry Date: 07/05/2011

Update: 03/28/2012

Link: http://ntc.doe.gov/shared/courses.aspx

BASIC TACTICAL ENTRY

T/E114 - PDU 40

This course covers the major elements comprising necessary knowledge and training for a Tactical Entry Specialist. It addresses selection, inspection, and proper manipulation of mechanical entry tools; identification and accomplishment of defeating barriers; target analysis in the review of target folders and intelligence prior to assault; communication; and breacher integration into the team. Lectures are reinforced by a series of practical skill-based activities designed to expose the student to realistic application of methods and techniques of employment. Activities follow a logical and progressive building-block approach that introduces the tools, methods of use, and integrated skill scenarios. Participants perform several graded (pass/fail) limited scope performance tests (LSPTs) and take one written examination requiring a score of at least 80%.

MEDICAL RELEASE: Site medical clearance forms MUST be on file with the National Training Center prior to attendance. DOE personnel must meet medical and fitness standards as mandated in 10 CFR 1046.

MANDATORY EQUIPMENT: Students must bring: load bearing vest, knee and elbow pads, Nomex gloves, department-issued long-sleeve shirt and long pants (Nomex flight suit recommended), leather above-the-ankle boots, approved eye protection, Level-III body armor, tactical gear with helmet.

NOTE: Dependent upon class size, some training days may run longer than stated in course schedule.

PREREQUISITE NOTE: Students will have attended either PFT-215, Basic Security Police Officer Training or TRF-100, Tactical Response Force 1 courses.

ID: PFT-405

Prerequisites: PFT-215 (Basic Security Officer Training)

Competencies: Physical Security

Delivery Type: Instructor-Led

Level: Not Specified

Length: 40 hours

Cost (Type): Not Specified

Provider: DOE>National Training Center

Entry Date: 07/05/2011

Update: 02/16/2012

Link: http://ntc.doe.gov/shared/courses.aspx

TACTICAL RESPONSE FORCE 1

T/E115 - PDU 45

This course provides standard basic training for the DOE Security Protection Officer II (SPO II) position upon entry into the DOE protective force community. TRF-1 will support the primary mission of the DOE Protective Force by providing training in the individual and team tactical combat skills necessary to protect safeguards and security interests from an armed terrorist threat. The scope of the course includes training in the use of handguns and rifles, an overview of advanced weapons, intermediate force and the DOE Force Continuum; field operations, recapture/ recovery support operations and defensive and emergency vehicle operations. Proficiency in these areas will be enhanced through situational training force-on-force exercises in support of initial classroom content delivery and firing range practice.

MEDICAL RELEASE: Site medical clearance forms MUST be on file with the National Training Center prior to attendance. DOE personnel must meet medical and fitness standards as mandated in 10 CFR 1046.

MANDATORY EQUIPMENT: Students must bring duty equipment, firearms and physical training gear, protective mask and filter, tactical flashlight and handcuffs, seasonal outdoor gear, groin protection, Nomex gloves and mat shoes. Mat/ wrestling-type shoes are recommended.

NOTE: Dependent upon class size, some training days may run longer than stated in course schedule.

ID: TRF-100

Prerequisites: TRF-100D (Introduction to Protective Force)

Competencies: Physical Security

Delivery Type: Instructor-Led

Level: Not Specified

Length: 400 hours

Cost (Type): Not Specified

Provider: DOE>National Training Center

Entry Date: 07/05/2011

Update: 02/16/2012

Link: http://ntc.doe.gov/shared/courses.aspx

TACTICAL RESPONSE FORCE 2

T/E116 - PDU 45

This course provides training and certification in skills and techniques required to effectively execute recapture/recovery and pursuit operations and to support interruption, interdiction, neutralization, containment, and denial strategies within the DOE environment as a member of a special response team (SRT). Students will develop close quarters marksmanship skills with handgun and rifle; close-quarters battle techniques; mounted, dismounted, and urban movement techniques; a variety of assault options; and mechanical and ballistic breaching techniques. Skills are applied in live-fire exercises and force-on-force scenarios under day and night conditions. Physical training occurs 3 days per week for the duration of the course.

REQUIREMENTS: Students must, prior to attendance, successfully qualify on the Tactical Response Force Combined Handgun/Rifle Qualification Course with a minimum score of 90 percent, be site-designated SPO IIs, meet medical and fitness standards as mandated in 10 CFR 1046, and file medical clearance forms with the National Training Center.

MANDATORY EQUIPMENT: Students must bring firearms and a duty training uniform (long sleeves required) appropriate to the season; boots providing ankle support; duty gear including belt, helmet, protective mask and filter, flashlight, flash-bang pouch, Nomex gloves, Level-III body armor and load-bearing equipment; knee pads/elbow pads; and a physical fitness training uniform appropriate to the season.

NOTE: Depending on class size, some training days may run longer than stated in course schedule.

AUDIENCE: DOE and DOE-contractor protective force personnel who will be assigned to the position of SPO III (SRT).

ID: TRF-200

Prerequisites: PFT-215 (Basic Security Officer Training) TRF-100 (Tactical Response Force 1)

Competencies: Physical Security

Delivery Type: Instructor-Led

Level: Not Specified

Length: 200 hours

Cost (Type): Not Specified

Provider: DOE>National Training Center

Entry Date: 07/06/2011

Update: 02/16/2012

Link: http://ntc.doe.gov/shared/courses.aspx

INTRODUCTION TO SAFEGUARDS AND SECURITY

T/E117 - PDU 2

This online course provides an overview of the DOE Safeguards and Security (S&S) Program, S&S training objectives and requirements, and the six S&S program elements: Program Planning and Management; Personnel Security; Physical Protection; Protective Force; Nuclear Material Control; and Accountability. Information Security SAS-101DE replaces CTA-101DC and is a required prerequisite for many S&S courses.

ID: SAS-101DE-Module 2

Prerequisites: None

Competencies: Information Security, Personnel Security

Delivery Type: Web-Based Training

Level: Not Specified

Length: 2 hours

Cost (Type): Not Specified

Provider: DOE>National Training Center

Entry Date: 07/06/2011

Update: 03/28/2012

Link: http://ntc.doe.gov/shared/courses.aspx

OPSEC FUNDAMENTALS

T/E118 - PDU 4/8

This correspondence course is available as a pdf download in the Online Learning Center (OLC) 2. Please download, print, and complete course per instructions. No registration is required. This introductory correspondence course provides an overview of the roles and responsibilities of the Department of Energy (DOE) or DOE-contractor facility security officer. The course emphasizes facility clearance requirements, personnel security, information security, incident reporting, and other related programs. The course references the National Industrial Security Program Operating Manual (NISPOM) and a comprehensive listing of DOE issuances. Successful completion of this course is measured by means of the six sets of end-of-lesson written test questions. Successful completion depends upon a minimum score of 80% on each end-of-lesson test. All documents related to this course can be found in their most current state at the following website: https://www.directives.doe.gov/

ID: OPSE-1300, OPSE-1300e,OPSE-1301 CBT

Prerequisites: None

Competencies: NSA>Interagency OPSEC Support Staff

Delivery Type: Web-Based Training/ Instructor-Led

Level: Not Specified

Length: 4 hours (web-based)/ 8 hours (instructor-led)

Cost (Type): No (Web-Based)

Provider: NSA>Interagency OPSEC Support Staff

Entry Date: 07/06/2011

Update: 02/16/2012

Link: https://www.iad.gov/ioss/department/opsec-fundamentals-course-opse1300-opse1301-opse1300e-10045.cfm

OPSEC AND PUBLIC RELEASE DECISIONS

T/E119 - PDU 8

This course addresses the operational security (OPSEC) issues that should be considered when reviewing information for public release and public access. Lessons can be applied to preparing information for release in all forms of media (e.g., print, web postings, public speeches). After completing this course, the student will be able to: edit information to be posted, written, and spoken by applying OPSEC principles; and achieve the originator's objective without compromising critical information. This course is specifically designed for individuals involved in determining what information should be released to the public, such as public affairs officers, web masters, Freedom of Information Act review staff, speech writers, speakers, classification review personnel, and OPSEC coordinators.

ID: OPSE-1500

Prerequisites: OPSEC Fundamentals course recommended

Competencies: Operations Security

Delivery Type: Platform/Web-Based Training

Level: Not Specified

Length: 1 day course

Cost (Type): Not Specified

Provider: NSA>Interagency OPSEC Support Staff

Entry Date: 07/06/2011

Update: 03/28/2012

Link: https://www.iad.gov/ioss/department/opsec-and-public-release-decisions-opse1500-10046.cfm

OPSEC ANALYSIS

T/E120 - PDU 16

The focus of this course is on the basic skills and knowledge needed by the operational security (OPSEC) practitioner. Upon completing this course, students will be able to apply the systems analysis methodology to their own organizations and activities, and identify sources of information and support materials. Lessons include:

* Tools for identification of critical information;
* Analysis of threat and resources to obtain threat information;
* Using the web for threat analysis;
* Identification of vulnerabilities, including the most common problem areas;
* Analysis of risk;
* Development and implementation of countermeasures, and assessment of residual risk; and
* Communicating analysis to leadership.

PREREQUISITE NOTE: Students will have attended either PFT-215, Basic Security Police Officer Training or TRF-100, Tactical Response Force 1 courses.

ID: OPSE-2380

Prerequisites: OPSEC Fundamentals (OPSE-1300) or equivalent

Competencies: Operations Security

Delivery Type: Platform

Level: Not Specified

Length: 2 days

Cost (Type): Not Specified

Provider: NSA>Interagency OPSEC Support Staff

Entry Date: 07/06/2011

Update: 02/16/2012

Link: https://www.iad.gov/ioss/department/opsec-analysis-course-opse2380-10047.cfm

OPSEC AND INTERNET BASED CAPABILITIES COURSE

T/E121 - PDU 16

This course discusses the nature of the Internet and how using various Internet technologies and devices may present unanticipated risks. Common practices such as communicating over the Internet, posting to public websites, and using third-party web services are rarely evaluated for their operational security (OPSEC) consequences. At the end of this course, the student will be better able to make informed choices of where and how to use the Internet and its related tools and services.

ID: OPSE-3500

Prerequisites: OPSEC Fundamentals (OPSE-1300) or equivalent

Competencies: Physical Security

Delivery Type: Platform

Level: Not Specified

Length: 2 days

Cost (Type): Not Specified

Provider: NSA>Interagency OPSEC Support Staff

Entry Date: 07/06/2011

Update: 02/16/2012

Link: https://www.iad.gov/ioss/department/web-risk-assessment-course-opse3500-10049.cfm

OPSEC ANALYSIS AND PROGRAM MANAGEMENT

T/E122 - PDU 32

The focus of this course is on the basic skills and knowledge needed to conduct an operational security (OPSEC) risk analysis (apply the 5 steps) and to implement an OPSEC program. The student is afforded the opportunity to apply OPSEC tools and lessons through a variety of practical exercises and case studies. Upon completing this course, students will be able to:

* Apply the systems analysis methodology to their own organizations and activities;
* Identify sources of information and support materials for OPSEC practitioners;
* Conduct an OPSEC analysis of a program, activity or operation;
* Market an OPSEC program;
* Write an organizational OPSEC policy; and
* Implement and manage an OPSEC program.

ID: OPSE-2500

Prerequisites: OPSEC Fundamentals (OPSE-1300) or equivalent

Competencies: Operations Security and Security Program Management

Delivery Type: Platform

Level: Not Specified

Length: 4 days

Cost (Type): Not Specified

Provider: NSA>Interagency OPSEC Support Staff

Entry Date: 07/06/2011

Update: 03/28/2012

Link: https://www.iad.gov/ioss/department/opsec-analysis-and-program-management-course-opse2500-10048.cfm

DNI/SSC CLASSIFICATION MANAGEMENT BRIEF

T/E123 - PDU 2

Provides 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, and derivative classification authorities and we will conclude with a classification exercise.

ID: Not Specified

Prerequisites: None

Competencies: Classification Management

Delivery Type: Instructor-Led

Level: Not Specified

Length: 3 hours

Cost (Type): No

Provider: ODNI-DNI Special Security Center

Entry Date: 07/06/2011

Update: 02/16/2012

Link: http://cryptome.org/2012/07/dni-ssc.pdf

LEADERSHIP ASSESSMENT PROGRAM LEVEL 1 FOR TEAM LEADERS AND EMERGING SUPERVISORS

T/E124 - PDU 40

This intensive, 5-day seminar will help you move into a leadership role or support you in the initial phase of your management career. You will complete personal assessment inventories and personality and temperament profiles, perform a case study analysis, and participate in various problem-solving activities. Thorough feedback and videotaped self-observation are integral aspects of the seminar. Assessment center specialist will help you identify your strengths and areas for improvement and provide you with confidential comprehensive guidance. You will leave with new insights to create a personal learning plan for continued leadership growth.

ID: Not Specified

Prerequisites: Not Specified

Competencies: Security Tools and Methods

Delivery Type: Instructor-Led

Level: Not Specified

Length: 5 days

Cost (Type): Yes

Provider: OPM> Federal Executive Institute

Entry Date: 07/06/2011

Update: 02/16/2012

Link: https://www.leadership.opm.gov/Programs/Individual-Assessment-and-Development/LAPL1/Index.aspx

LEADERSHIP ASSESSMENT PROGRAM LEVEL 2

T/E125 - PDU 40

This intensive 5-day program provides supervisors and managers with new insights into their leadership strengths and helps uncover areas for potential improvement. As you learn the factors critical to successful leadership, you will be evaluated in several leadership competency areas and coached to create a Leadership Development Plan (LDP). Using lectures, exercises, assessments and individual feedback, you will acquire the critical strategies you need to improve your leadership performance and achieve organizational success.

All participants meet for a private half-day session with a professional executive coach to discuss strengths, areas for development, and next steps on your Government career path.

ID: Not Specified

Prerequisites: Not Specified

Competencies: Security Tools and Methods

Delivery Type: Instructor-Led

Level: Not Specified

Length: 5 days

Cost (Type): Yes

Provider: OPM>Federal Executive Institute

Entry Date: 07/06/2011

Update: 02/16/2012

Link: https://www.leadership.opm.gov/Programs/Individual-Assessment-and-Development/LAPL2/Index.aspx

LEADING STRATEGICALLY: FROM VISION TO PERFORMANCE

T/E126 - PDU 24

Developing a new strategic plan is one of the most common (and essential) ways an organization addresses change. Unfortunately, "wondering what went wrong" is an all-too common follow-up. How do high-performing organizations identify and complete the vital steps between planning and implementation?

This program offered by the Federal Executive Institute (FEI) provides practical skills for leaders in rapidly changing environments. Through large- and small-group discussions and exercises, you will identify changes your organization must undertake to realize its vision. You will learn the best ways to develop, communicate, and refresh your organizational vision through engaging your staff, then focusing on methods to evaluate performance on each goal as the change effort initiative progresses.

ID: Not Specified

Prerequisites: None

Competencies: Security Tools and Methods

Delivery Type: Instructor-Led

Level: Not Specified

Length: 3 days

Cost (Type): Yes

Provider: OPM> Federal Executive Institute

Entry Date: 07/06/2011

Update: 02/16/2012

Link: https://www.leadership.opm.gov/Programs/Organizational-Leadership-for-Executives/EXE0005/Index.aspx

CRISIS LEADERSHIP WORKSHOP

T/E127 - PDU 40

Despite great improvements in crisis prevention and strategic management capabilities, actual crises often elude the best of strategic plans. How do you lead when your plans are insufficient, the unexpected occurs, or your core values are threatened? How do you respond to unanticipated situations when time is of the essence and planned approaches don't work? Are you equipped to be flexible, to delegate responsibility, and marshal resources quickly?

The Crisis Leadership Workshop helps you identify emergency situations, assess your own biases under pressure, manage new information effectively, make informed decisions, and create and lead a crisis team. Through case studies, films, interactive exercises and simulated crises, you will learn to identify your personal strengths in relating to others when you are threatened, as well as how to manage relationships before, during, and after a crisis. By sharing your crisis leadership experience with others, you will also develop an invaluable network of colleagues across agencies for ongoing support.

ID: Not Specified

Prerequisites: None

Competencies: Incident Response

Delivery Type: Instructor-Led

Level: Not Specified

Length: 5 days

Cost (Type): Yes

Provider: OPM>Management Development Center

Entry Date: 07/06/2011

Update: 02/16/2012

Link: https://www.leadership.opm.gov/Programs/Specialized-Skills/CMS/Index.aspx

EXECUTIVE DEVELOPMENT SEMINAR: LEADING CHANGE

T/E128 - PDU 45

Designed for senior Federal and other public sector managers, this seminar focuses on developing and transitioning senior managers from technical, division-level work to strategic, agency-level leadership positions. You will be challenged to think about your organization's big picture as it relates to policy, strategic planning, leadership, and change. Enhance your ability to communicate and interact positively with constituencies. You will identify and plan for internal and external politics that impact your vision, mission, and organization.

Through a group project, you will learn the fundamentals and finer aspects of strategic thinking, strategic planning, and political research. You will also examine how policy is made and how to maximize the interests of all concerned parties. Participants are expected to have completed a 360-degree leadership assessment prior to this seminar. If not, a 360 assessment will be included.

ID: Not Specified

Prerequisites: None

Competencies: External Awareness, Interpersonal Skills, Oral Communication, Political Savvy, Strategic Thinking

Delivery Type: Instructor-Led

Level: Not Specified

Length: 2 weeks

Cost (Type): Yes

Provider: OPM>Management Development Center

Entry Date: 07/06/2011

Update: 02/16/2012

Link: https://www.leadership.opm.gov/Programs/Executive-Leadership-Development/EDS/Index.aspx

MANAGEMENT DEVELOPMENT SEMINAR I: LEADING FROM THE MIDDLE

T/E129 - PDU 45

Managers, especially those of supervisors or those with oversight of groups and programs, have a great deal of responsibility for Government's productivity and performance. As a key leader in your organization, your challenges are complex and your leadership is integral to your agency's success.

Whether you are a new middle manager or an experienced first-line supervisor, you need to think critically and develop your communications skills. This nine-day, residential program targets essential management competencies through individual assessments, readings, small group activities, real-world experiences, and stimulating class discussions. During this seminar, you will:

* Learn and apply tools for improving skills in conflict resolution and problem solving
* Increase your self-knowledge and leadership capacity through critical thinking, exploring strengths theory, and examining change models
* Solve a real management challenge through a small group action learning process
* View your leadership role through Constitutional values and courageous relationships

ID: Not specified

Prerequisites: None

Competencies: Classification Management

Delivery Type: Instructor-Led

Level: Not Specified

Length: 2 weeks

Cost (Type): Yes

Provider: OPM>Management Development CenterEntry

Date: 07/06/2011

Update: 02/16/2012

Link: https://www.leadership.opm.gov/Programs/Management-and-Supervisory-Skills/MDS1/Index.aspx

PROJECT MANAGEMENT PRINCIPLES

T/E130 - PDU 40

Project Management Principles (PMP) will set you apart as a skilled leader in today's increasingly project-driven workplace, providing you with the business, communication, and leadership skills needed to manage projects to achieve organizational goals.

An intensive, 5-day program, this course illuminates the project leadership equation by providing a solid foundation in project management principles, specialized tools, and best and current practices used by experienced project managers. You will learn and apply key concepts about managing a project, such as scope management, chartering, work breakdown, scheduling, accountability, communication planning, earned value, risk evaluation, and Critical Path Method (CPM).

Using a classic project management model, you will synthesize your learning and gain operational experience by presenting a real world project plan—all under the guidance of certified project managers and expert facilitators. The curriculum is aligned with the internationally recognized Project Management Institute's Body of Knowledge (PMBOK), which serves as the guide to key terms and in-depth process descriptions.

ID: Not Specified

Prerequisites: None

Competencies: Security Tools and Methods

Delivery Type: Instructor-led

Level: Not Specified

Length: 1 week

Cost (Type): Yes

Provider: OPM>Management Development Center

Entry Date: 07/06/2011

Update: 02/16/2012

Link: https://www.leadership.opm.gov/Programs/Specialized-Skills/PMP/Index.aspx

INTRODUCTION TO RISK MANAGEMENT

T/E131 - PDU 0.5

This course is designed to provide an introduction to the five-step Risk Management process.

ID: GS150.16

Prerequisites: None

Competencies: Incident Response, Vulnerabilities Assessment and Management

Delivery Type: Web-Based Training

Level: Introductory

Length: 30 minutes

Cost (Type): No

Provider: DoD>DSS>CDSE

Entry Date: 07/06/2011

Update: 02/16/2012

Link: http://www.dss.mil/cdse/catalog/elearning/GS150.html

INTRODUCTION TO CRITICAL PROGRAM INFORMATION AWARENESS

T/E132 - PDU 1.5

This is an introductory course for DoD or Defense Industrial personnel working on programs which may contain Critical Program Information. The information includes an explanation of how CPI identification and required continuous security protection procedures fit into the Defense Acquisition Life Cycle. The training covers the purpose and identification process of CPI. It provides policy guidance, steps taken to identify CPI (threat assessment, vulnerabilities, risk management), lists required procedures to support CPI, and review of the Program Protection Plan and countermeasure requirements.

ID: C120.16

Prerequisites: None

Competencies: Vulnerabilities Assessment and Management, Incident Response

Delivery Type: Web-Based Training

Level: Introductory

Length: 90 minutes

Cost (Type): No

Provider: DoD>DSS>CDSE

Entry Date: 07/06/2011

Update: 03/28/2012

Link: http://dssa.dss.mil/seta/courses.html

DISAM- INTERNATIONAL PROGRAMS SECURITY REQUIREMENTS-IPSR-OLL

T/E133 - PDU 24

The International Programs Security Requirements Course On-Line (IPSR-OL) course covers the principles and procedures that facilitate international technology transfer, export controls, and foreign disclosure. Specific lessons discuss the acquisition process for international program security, controlled unclassified and foreign government information, the National Disclosure Policy, and the International Traffic in Arms Regulations (ITAR). The export approval and license process is covered along with the role of the Defense Security Service (DSS). Other topics include visits and assignments of foreign nationals, Multinational Industrial Security Working Group (MISWG) documents, Committee on Foreign Investment in the United States (CFIUS) and Foreign Ownership, Control or Influence (FOCI), and the transfer of classified information.

ID: IN112.06

Prerequisites: None

Competencies: Program Security

Delivery Type: Web-Based Training

Level: Not specified

Length: 24 hours

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 07/06/2011

Update: 03/28/2012

Link: http://dssa.dss.mil/seta/courses.html

DOD FOREIGN DISCLOSURE ORIENTATION

T/E134 - PDU 2.5

This course helps personnel gain familiarity with the Department of Defense (DoD) Foreign Disclosure Program. Students learn how foreign disclosure of classified military information affects and enhances DoD operations and activities. The course also helps students understand the laws, executive orders, and policies and procedures necessary for performing the critical task of foreign disclosure. Foreign Disclosure with allied and other friendly countries is an increasingly important part of our national security and defense acquisition and operational strategies. International armaments cooperation, in its many forms, enhances interoperability, stretches declining Defense budgets, and preserves Defense industrial capabilities. Equally important is the recognition that coalitions are the preferred way for U.S. forces to confront major regional and global security issues. This requires the United States to consider the national security benefits of sharing technology, classified military information, and controlled unclassified information with allies, other friendly countries, and coalition partners.

ID: GS190.06

Prerequisites: None

Competencies: Information Security, Classification Management, Personnel Security

Delivery Type: Web-Based Training

Level: Not Specified

Length: 2 hours 30 minutes

Cost (Type): Not Specified

Provider: DoD > DSS > CDSE

Entry Date: 07/06/2011

Update: 02/16/2012

Link: http://dssa.dss.mil/seta/courses.html

INTRODUCTION TO DOD FOREIGN DISCLOSURE

T/E135 - PDU .5

This course introduces personnel to the Department of Defense (DoD) Foreign Disclosure Program. Students acquire knowledge concerning the basic concepts of foreign disclosure in international cooperative and operational environments, specifically in international programs and activities that involve disclosure of U.S. classified military information (CMI) to foreign governments and international organizations. In addition, this course introduces the National Security and National Military Strategies of the United States and their impact on foreign disclosure decisions.

ID: GS200.06

Prerequisites: None

Competencies: Information Security, Classification Management, Personnel Security

Delivery Type: Web-Based Training

Level: Not specified

Length: 30 minutes

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 07/06/2011

Update: 03/28/2012

Link: http://dssa.dss.mil/seta/courses.html

T/E136 - PDU 2

DoD Generic Research, Development, Test and Evaluation (RDT&E) Information Exchange Program (IEP), a new International Armaments Cooperation (IAC) module, is a two-hour training module offered to ensure that acquisition workforce members understand the IEP, why they should use the IEP and be able to execute IEP information exchanges with expertise, responsibility and accountability.

ID: IN104.06

Prerequisites: None

Competencies: Information Security, Information Assurance/Cyber Security

Delivery Type: Web-Based Training

Level: Not Specified

Length: 2 hours

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 07/06/2011

Update: 02/16/2012

Link: http://dssa.dss.mil/seta/courses.html

T/E137 - PDU 1

This module ensures that all required acquisition workforce personnel comprehend Army-specific Information Exchange Program (IEP) annex development, coordination, negotiation, and execution changes in policy and procedures. This training module includes:

* Introduction to Army-Specific IEP
* The Army-specific IEP requirements
* The use of U.S. Army International Online (IOL) International Armaments Cooperation (IAC) agreements, annexes and activities development, coordination and management system for developing the Templates for the IEP Annex Package, and
* IEP Army IEP decentralization of the IEP annex development, coordination, negotiation, and conclusion process.

ID: IN101.06
Prerequisites: None
Competencies: Program Security
Delivery Type: Web-Based Training

Level: Not Specified
Length: 1 hour
Cost (Type): No
Provider: DoD > DSS > CDSE
Entry Date: 06/06/2011
Update: 02/16/2012

Link: http://dssa.dss.mil/seta/courses.html

DAU-INTERNATIONAL ARMAMENTS COOPERATION, PART 2 CLI 002

T/E138 - PDU 2

This module forms part two of a three-part curriculum focused on International Armaments Cooperation. The learner should complete module one before taking module two. Each module in the International Armaments Cooperation series prepares learners to complete instructor-led, classroom-based modules conducted by the Defense Acquisition University. Students are encouraged to complete each of the three modules in order for maximum benefit. The average cumulative time for each module completion is 2 hours.
This module has been revised to:

* Update the International Agreements' and the Foreign Comparative Testing (FCT) program's policies and processes.
* Reflect the newly entitled and revamped Defense Research, Development, Test and Evaluation (RDT&E) Information Exchange Program (IEP).
* Expand Defense Personnel Exchanges and Assignments Lesson beyond the Engineer and Scientists Exchange Program (ESEP) to also include the Administrative and Professional Personnel Exchange Program (APEP) and Cooperative Programs/Projects Personnel (CPP) program.

ID: IN102.06
Prerequisites: None
Competencies: Program Security
Delivery Type: Web-Based Training

Level: Not Specified
Length: 2 hours
Cost (Type): No
Provider: DoD > DSS > CDSE
Entry Date: 07/06/2011
Update: 02/16/2012

Link: http://dssa.dss.mil/seta/courses.html

DAU-INTERNATIONAL ARMAMENTS COOPERATION, PART 3, CLI 003

T/E139 - PDU 2

The International Armaments Cooperation (IAC) Part 3 is the final in a three-part curriculum focused on International Armaments Cooperation. Learners should complete modules one and two before taking part three. Each module in the International Armaments Cooperation series prepares learners to complete instructor-led, classroom-based modules conducted by the Defense Acquisition University. Students are encouraged to complete each of the three modules in order to receive maximum benefit.
This reconstructed module updates lessons on:

* Defense Trade and Industrial Cooperation
* Cooperative Logistics, and
* Replaces the lesson on international environmental cooperation with an important lesson on Security and Technology Transfer Requirements for IAC.

This course is based on the Department of Defense (DoD) Handbook, International Armaments Cooperation Handbook.

ID: IN103.06
Prerequisites: None
Competencies: Program Security
Delivery Type: Web-Based Training

Level: Not Specified
Length: 2 hours
Cost (Type): No
Provider: DoD > DSS > CDSE
Entry Date: 07/06/2011
Update: 02/16/2012

Link: http://dssa.dss.mil/seta/courses.html

DAU-TECHNOLOGY TRANSFER AND EXPORT CONTROL FUNDAMENTALS CM 036

T/E140 - PDU 2

This module is intended to provide awareness of Fundamentals of Technology Transfer and Export Control International Security and Program Protection and Planning Process Role of the Program Manager.

ID: IN07.06

Prerequisites: None

Competencies: Information Security, Program Security, Security Program Management

Delivery Type: Web-Based Training

Level: Not Specified

Length: 2 hours

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 07/06/2011

Update: 03/28/2012

Link: http://dssa.dss.mil/seta/courses.html

DISAM-SECURITY ASSISTANCE MANAGEMENT ORIENTATION SAM-OC

T/E141 - PDU 24

SAM-OC is an online distance-learning course that contains 7 lessons on topics in functional areas of security assistance management. In progressing through each lesson the student will be able to view graphics with key instructional points; listen to the instructor narrate text and address points on a graphic; and follow along by reading the text of the instructor's remarks at the bottom of the screen.

ID: IN110.06

Prerequisites: None

Competencies: Security Program Management

Delivery Type: Web-Based Training

Level: Not Specified

Length: 24 hours

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 07/06/2011

Update: 02/16/2012

Link: http://dssa.dss.mil/seta/courses.html

DISAM-SECURITY COOPERATION OFFICER ORIENTATION SCM-OC

T/E142 - PDU 20-25

The purpose of the Security Cooperation Officer's Orientation Courses Course Schedule: (SCM-OC) are to provide interim orientation on security cooperation/ assistance to DoD personnel on orders to serve in a security cooperation organization (SCO) overseas and who are unable to attend DISAM prior to deployment.

ID: IN111.06

Prerequisites: None

Competencies: Security Program Management

Delivery Type: Web-Based Training

Level: Not Specified

Length: 20-25 hours

Cost (Type): No

Provider: DoD>DSS>CDSE

Entry Date: 07/06/2011

Update: 03/28/2012

Link: http://dssa.dss.mil/seta/courses.html

DOD ADVANCED PERSONNEL SECURITY ADJUDICATION

T/E143 - PDU 36

This course provides in-depth study of adjudication policy guidelines and the basis for and application of due process in unfavorable personnel security determinations. The course emphasizes evaluation and resolution of complex multiple and sensitive issue cases, the actions as well as agencies and related requirements involved.

ID: PS301.01
Prerequisites: None
Competencies: Not Specified
Delivery Type: Instructor-Led

Level: Not Specified
Length: 4.5 days
Cost (Type): No
Provider: DoD > DSS > CDSE
Entry Date: 07/06/2011
Update: 03/28/2012

Link: http://dssa.dss.mil/seta/courses.html

INTRODUCTION TO DOD PERSONNEL SECURITY ADJUDICATION

T/E144 - PDU 3

This course has been updated from its formally named course - DoD Personnel Security Adjudications Independent Study Course.

Explains DoD Personnel Security Program basics and introduces several key concepts covered in the resident DoD Personnel Security Adjudications (PS101.01) course. This course is prerequisite training for persons approved to attend the DoD Personnel Security Adjudications Course (PS101.01).

ID: PS001.18
Prerequisites: None
Competencies: Personnel Security
Delivery Type: Web-Based Training

Level: Not Specified
Length: 3 hours
Cost (Type): No
Provider: DoD > DSS > CDSE
Entry Date: 07/06/2011
Update: 02/16/2012

Link: http://dssa.dss.mil/seta/courses.html

FUNDAMENTALS OF INDUSTRIAL SECURITY LEVEL ONE (FISL 1)

T/E145 - PDU

This course provides the fundamental knowledge of the National Industrial Security Program (NISP). The course is structured for basic levels of achievement qualifying the student to perform non-complex survey and inspection of actions independently. This is accomplished through a combination of on-the-job training, mentoring, online courseware and structured research, writing, and performance activities. The course prepares the individuals for the FISL 2 course, which is a follow-on application-based course that builds on the individual's knowledge and skills acquired in FISL 1.

ID: IS115.CU

Prerequisites: DSS Employees Only

Competencies: Not Specified

Delivery Type: Blended Learning Course

Level: Introductory

Length: 4-6 months

Cost (Type): None

Provider: DoD > DSS > CDSE

Entry Date: 03/15/2012

Update:

Link: http://www.dss.mil/cdse/catalog/elearning/index.html

FUNDAMENTALS OF INDUSTRIAL SECURITY LEVEL TWO

T/E146 - PDU

This course builds upon the knowledge and skills learned in the Fundamentals of Industrial Security Level 1, and trains the student to perform inspections of non-complex possessing facilities, which are approved to store classified material under the NISP.

ID: IS210.01

Prerequisites: DSS Employees Only

IS115.CU

Competencies: Not Specified

Delivery Type: Instructor-Led

Level: Intermediate

Length: 2 weeks

Cost (Type): None

Provider: DoD > DSS > CDSE

Entry Date: 03/15/2012

Update:

Link: http://www.dss.mil/cdse/catalog/elearning/index.html

CERTIFICATION AND ACCREDITATION REVIEWER COURSE

T/E147 - PDU

This instructor-led course is intended for Industrial Security Representatives (IS Reps) to expand their skills and augment field ISSPs related to the Certification and Accreditation (C&A) of Single User Stand Alone (SUSA), Multiple User Stand Alone (MUSA), and simple Peer-to-Peer (P2P) Information Systems. The course focuses on the desktop review, on-site inspection, and advise and assist role of the C&A Reviewer. Close attention is given to the baseline standards for a Microsoft Windows XP operating system, including how to read and interpret audit logs. Participants will also be given an opportunity to practice their interview and writing skills, conduct an on-site validation of a P2P information system, and annual inspection of a MUSA information system.

ID: IS220.01

Prerequisites: Basic Application of Information Assurance for the C&A Reviewer Course

Competencies: Not Specified

Delivery Type: Instructor-led

Level: Not Specified

Length: 9 days

Cost (Type): None

Provider: DoD > DSS > CDSE

Entry Date: 03/15/2012

Update:

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

T/E148 - PDU

Still Under Development

ID:
Prerequisites:
Competencies:
Delivery Type:

Level: Not Specified
Length:
Cost (Type): None
Provider: DoD > DSS > CDSE
Entry Date:
Update:

Link: http://www.dss.mil/cdse/catalog/elearning/index.html

INDUSTRIAL SECURITY FACILITIES DATABASE FOR DSS USERS

T/E149 - PDU

This course provides step-by-step instructions on the use of the Industrial Security Facilities Database (ISFD). Students practice populating and manipulating the ISFD in a virtual classroom environment that simulates all the functionality of the real-time database.

ID: IS110.06

Prerequisites: DSS Employees Only
None

Competencies: Not Specified

Delivery Type: Web-Based Training

Level: Not Specified

Length: 8 hours

Cost (Type): None

Provider: DoD > DSS > CDSE

Entry Date: 03/15/201

Update:

Link: http://www.dss.mil/seta/enrol/stepp.html

E-FCL FOR DSS USERS

T/E150 - PDU 1

This course provides Industrial Security personnel with an introduction to the Defense Security Service (DSS) electronic Facility Security Clearance (e-FCL) application. The course provides instruction on how to navigate and use the DSS e-FCL system to process facility clearance and FOCI information received by contractors through use of instruction, simulations, and hands-on practice in a virtual classroom environment.

ID: IS352.06

Prerequisites: DSS Employees Only

None

Competencies: Not Specified

Delivery Type: Web-Based

Level: Not Specified

Length: 1.5 hours

Cost (Type): None

Provider: DoD > DSS > CDSE

Entry Date: 03/15/2011

Update:

Link: http://www.dss.mil/seta/enrol/stepp.html

T/E151 - PDU

Still Under Development

ID:
Prerequisites:
Competencies:
Delivery Type:

Level:
Length:
Cost (Type): None
Provider: DoD > DSS > CDSE
Entry Date:
Update:

Link: http://www.dss.mil/cdse/catalog/elearning/index.html

WRITING AND COMMUNICATION SKILLS FOR SECURITY PROFESSIONALS

T/E152 - PDU 45

This course is an exploration of the skills and behaviors that contribute to success in oral and written communications. It is focused on the specific written and oral communication skills needed by a DoD security professional.

ID: ED201.01

Prerequisites: Freshman English from a regionally accredited institution or equivalent is recommended.

Competencies: Not Specified

Delivery Type: Instructor-Led

Level: Not Specified

Length: 16 Weeks

Cost (Type): None

Provider: DoD > DSS > CDSE

Entry Date: 05/15/2012

Update:

Link: http://www.dss.mil/cdse/catalog/elearning/ED201.html

SECURITY AS AN INTEGRAL PART OF DOD PROGRAMS

T/E153 - PDU 45

This course is a comprehensive study of Defense Security as a cross-disciplinary function that supports the missions of DoD commands and agencies. This course addresses DoD security as a profession and reviews the scope of the security essential body of work. This course addresses the emerging role of the multi-disciplinary security generalist as a career path.

ID: ED501
Prerequisites: None
Competencies: Not Specified
Delivery Type: Web-Based Training

Level: Not Specified
Length: 16 Weeks
Cost (Type): None
Provider: DoD > DSS > CDSE
Entry Date: 05/15/2011
Update:

Link: http://www.dss.mil/cdse/catalog/elearning/ED501.html

ORGANIZATIONAL CONSIDERATIONS IN APPLYING SECURITY WITHIN THE FEDERAL AND DOD BUREAUCRACY

T/E154 - PDU 45

This course presents an in-depth look at how to work within the Federal and DoD bureaucracy to accomplish security missions and objectives. The course will address how security professionals can support military operations and DoD programs most effectively. The course includes in-depth study of the missions, jurisdiction of, and limitations upon the many agencies and offices involved in security policy and programs.

ID: ED502
Prerequisites: None
Competencies: Not Specified
Delivery Type: Web-Based Training

Level: Not Specified
Length: 16 Weeks
Cost (Type): None
Provider: DoD > DSS > CDSE
Entry Date: 05/15/2012
Update:

Link: http://www.dss.mil/cdse/catalog/elearning/ED502.html

CONSTITUTIONAL LAW AND ITS APPLICATION TO DOD SECURITY

T/E155 - PDU 45

This course examines the origins of, distribution of, and limitations upon governmental authority under the Constitution of the United States. It includes study of the doctrine of Legislative, Judicial, and Executive action; the powers of Congress, the courts, and the President; and the limitations on Federal and State governmental powers. The course also focuses on Congressional power, Executive power, and judicial protection against the abuse of Government power in violation of rights, liberties, privileges, or immunities conferred by the Constitution. In particular, the course examines specific cases that have had an impact on DoD security programs.

ID: ED503
Prerequisites: None
Competencies: Not Specified
Delivery Type: Web-Based Training

Level: Not Specified
Length: 17 Weeks
Cost (Type): None
Provider: DoD > DSS > CDSE
Entry Date: 05/15/2012
Update:

Link: http://www.dss.mil/cdse/catalog/elearning/ED503.html

UNDERSTANDING ADVERSARIES AND THREATS TO THE UNITED STATES AND DOD

T/E156 - PDU 45

This course specifically addresses the intentions and capabilities of the three to five most significant adversaries to the United States and to the Department of Defense (DoD). It also examines the multifaceted concept of threat: Who presents a threat? What are internal and external threats? What is being threatened? Who can provide a threat assessment? The course addresses counterintelligence, counterterrorism, insider threats, and threats to critical information systems. In addition, this course covers such critical threats as embezzlement, physical sabotage, violence in the workplace by disgruntled employees, and others that must be addressed by the senior security manager. The course familiarizes students with government and non-government sources of reliable threat information.

ID: ED504

Prerequisites: DoD Derivative Classification (IF103.16 and IF103.06)

Marking Classified Information (IF105.16 and IF105.06)

Integrating CI and Threat Awareness into Your Security Program (CI010.16 and CI010.06)

Secret Clearance

Competencies:

Delivery Type: Web-Based Training

Level: Not Specified
Length: 16 Weeks
Cost (Type): None
Provider: DoD > DSS > CDSE
Entry Date: 05/15/2012
Update:

Link: http://www.dss.mil/cdse/catalog/elearning/ED504.html

T/E157 - PDU 45

This course presents the specific statutes, regulations, and Executive Orders driving the establishment and implementation of Department of Defense (DoD) and Federal security programs.

ID: ED601
Prerequisites: None
Competencies:
Delivery Type: Web-Based Training

Level: Not Specified
Length: 16 Weeks
Cost (Type): None
Provider: DoD > DSS > CDSE
Entry Date: 05/15/2012
Update:

Link: http://www.dss.mil/cdse/catalog/elearning/ED601.html

CHALLENGES IN ANALYZING AND MANAGING RISK

T/E158 - PDU 45

This course provides a comprehensive study of risk management as used by high-level management officials to support decision making. The course addresses risk management theory and DoD risk management practice and builds comfort with risk management decision-making methodology in dealing with imminent security threats. During the semester, students complete a series of assignments involving application of risk management to a specific mission or project at their agency. At course conclusion, students return to the Center for Development of Security Excellence (CDSE) to present their risk management project to senior leaders in the affected organization.

ID: ED602

Prerequisites: Risk Management for DoD Security Programs GS102.16/06

Integrating Counterintelligence and Threat Awareness Into Your Security Program CI010.16

DoD Derivative Classification IF103.16/06

Marking Classified Information IF105.16/06

Competencies: Not Specified

Delivery Type: Web-Based Training

Level: Not Specified

Length: 17 Weeks

Cost (Type): None

Provider: DoD > DSS > CDSE

Entry Date: 05/15/2011

Update:

Link: http://www.dss.mil/cdse/catalog/classroom/ED602.html

INTERAGENCY COMMUNICATION FOR STABILITY OPERATIONS

T/E159 - PDU 30

The ability to communicate effectively is a vital tool for interagency leaders working stability operations. Messages must be conveyed rapidly and with due clarity in order to generate the strategic effect required. Leaders must develop their ability to harness and leverage various forms of communication media to convey their intent. In a seminar environment, students will focus on real-life stability operation case studies and role play appointments to practice and improve their abilities to brief, present questions, interview and actively listen. Students will also learn the pros and cons of various types of communication media.

ID: 6968

Prerequisites: Not Specified

Competencies: Communications
Security

Delivery Type: Instructor-Led

Level: Not Specified
Length: Semester
Cost (Type): Yes
Provider: NDU>CISA
Entry Date: 06/29/2011
Update: 03/27/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

DYNAMICS OF COUNTERTERRORISM

T/E160 - PDU 45

This course provides an examination of the counterterrorism response at the national and international levels. Case studies and use of primary documents allow students to examine the implications for appropriate and comprehensive response. Students analyze strategic response by exploring the appropriate campaigns constructed to neutralize components of insurgent strategy. As a culminating exercise, students develop a national counterterrorism plan.

ID: 6976
Prerequisites: Not Specified
Competencies: Counterintelligence
Delivery Type: Instructor-Led

Level: Not Specified
Length: Semester
Cost (Type): Yes
Provider: NDU>CISA
Entry Date: 06/29/2011
Update: 03/27/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

COMBATING TERRORISM STRATEGIES AND POLICIES

T/E161 - PDU 45

This course examines the ongoing challenge to U.S. national security posed by the threat of international terrorism. The course will examine the causes of the rise of the global terrorist threat, the motives and methods of the terrorists, and the ways in which the United States is waging war to prevent future terror attacks and safeguard the homeland. Readings include primary source documents related to the continuing conflict, as well as classics in terrorism literature.

ID: 6990
Prerequisites: Not Specified
Competencies: Counterintelligence
Delivery Type: Instructor-Led

Level: Not Specified
Length: Semester
Cost (Type): Yes
Provider: NDU>CISA
Entry Date: 06/29/2011
Update: 03/27/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

LAW ENFORCEMENT VS. INTELLIGENCE: THE ROLE OF INTERNAL SECURITY ORGANIZATIONS

T/E162 - PDU 45

This course examines how the Internal Security Establishments (ISEs) of five democratic nations — the U.S, U.K., France, Germany, and Israel — are carrying out modifications in their structure and methods in the post-9/11 era. In so doing, the course attempts to understand the problems faced in bringing about these changes, chief among them being that of balancing freedom and security. While the focus will be primarily on tactical and operation levels of counter-terrorism, the course will also analyze business plans, organizational structure, operational methods, and threat assessment criteria. The ultimate objective in this course is to learn more about how a nation under threat from international terrorism builds and maintains an effective and efficient domestic security infrastructure.

ID:	6989	**Level:**	Not Specified
Prerequisites:	Not Specified	**Length:**	Semester
Competencies:	Counterintelligence	**Cost (Type):**	Yes
Delivery Type:	Instructor-Led	**Provider:**	NDU>CISA
		Entry Date:	06/29/2011
		Update:	03/27/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

STRATEGIC INTELLIGENCE AND THE WAR ON TERRORISM

T/E163 - PDU 45

This course offers an intellectual and historical foundation for understanding the American intelligence community, the intelligence process, and its role in national security policy. It examines how intelligence agencies operate in a democratic society, how perspectives differ between providers and users of intelligence, and the role of Congressional oversight. To evaluate strengths and weaknesses of strategic intelligence, students focus on its role in the Cold War, the 1990-91 Gulf War, the 1998 strikes against al-Qaeda in Afghanistan and Sudan, the 1999 Kosovo War, the failure of strategic warning prior to September 11, 2001, and the U.S. invasions of Afghanistan in 2001 and Iraq in 2003. Lessons derived from these case studies equip students to separate fact from fiction in the ongoing debate, and to evaluate reforms proposed or underway. Such analytical rigor is essential for students of the American policy process as well as their foreign counterparts in a global coalition in the War on Terrorism.

ID: 6994

Prerequisites: Not Specified

Competencies: Not Specified

Delivery Type: Instructor-Led

Level: Not Specified

Length: Semester

Cost (Type): Yes

Provider: NDU>CISA

Entry Date: 06/29/2011

Update: 03/27/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

INTELLIGENCE IN COUNTERINSURGENCY OPERATIONS

T/E164 - PDU 30

Intelligence is a critical part of political/military conflict at the tactical through the strategic levels of operations. This course will consider intelligence activities from the perspective of commanders and non-intelligence staff officers conducting counterinsurgency operations. It will focus on the capabilities and limitations of intelligence, as well as the challenges of using intelligence to support policy and to guide the instruments of national power, including military force. Detailed historical and more limited contemporary case studies will provide lessons of successful and unsuccessful uses of intelligence in counterinsurgency operations.

ID: 6915
Prerequisites: Not Specified
Competencies: Counterintelligence
Delivery Type: Instructor-Led

Level: Not Specified
Length: Semester
Cost (Type): Yes
Provider: NDU>CISA
Entry Date: 06/30/2011
Update: 03/27/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

GEOSTRATEGY

T/E165 - PDU 2

Geostrategy is a required core course in the Master of Arts in Strategic Security Studies (MASSS) program. This course is designed to enable students to define and critically analyze the dimensions of the contemporary security environment. In Section I, students will explore the concept of security and how that concept has changed in the post-Cold War and post-9/11 environments. A key feature of the contemporary security environment is the proliferation of actors both in number and type. In Section II, students will examine a complex array of new actors and new linkages among them. These actors include not only states, but also international organizations, armed non-state actors, and super-empowered individuals and groups. As the number of actors has proliferated, so too has the number of security challenges. In Section III, the course examines the key dynamics and threats that define the contemporary security environment. Students will focus on globalization, scarcity, state failure, democratization, ethnic and sectarian conflict, cyber attacks, and weapons of mass destruction (WMD) proliferation. In the final section of the course, students will examine the actors and security dynamics explored in Sections I, II, and III across Africa, South and Central America, the Middle East and the Maghreb, Central and Southwest Asia, Southeast Asia, and Europe. The purpose of the course is not to create regional experts but to develop a working knowledge of the international security context that is essential for creating, analyzing, and carrying out national security strategy and policy.

ID: 6920
Prerequisites: Not Specified
Competencies: Not Specified
Delivery Type: Instructor-Led

Level: Masters Program
Length: Semester
Cost (Type): Yes
Provider: NDU>CISA
Entry Date: 07/00/2011
Update: 03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

POWER, IDEOLOGY AND LEGITIMACY

T/E166 - PDU 45

This course will examine the genesis, conceptual development, and relationship between power and legitimacy, focusing particularly on how ideologies are used either to justify rule or oppose the established order. The initial part of the course will focus on the greater debates of political philosophy relevant to the meaning of these and other intimately related concepts, such as justice and the nature of the sovereign. The second section will revisit the different interpretations given to these concepts, looking at how they are operationalized throughout time. Finally, an in-depth analysis of radical Islam will help answer two questions: How do ideology, legitimacy, and power interact with the current 36 challenge posed by religiously inspired, armed, non-state actors whose goal is to fundamentally alter the current international system? How can the state employ its sources of power and legitimacy to approach this challenge?

ID:	6929
Prerequisites:	Not Specified
Competencies:	Not Specified
Delivery Type:	Instructor-Led

Level:	Masters
Length:	Semester
Cost (Type):	Yes
Provider:	NDU>CISA
Entry Date:	07/06/2011
Update:	03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

T/E167 - PDU 45

This course examines from a theoretical and historical perspective the military institutions of the U.S. as they relate to the democratic state. It covers such topics as the concept of the military profession and the professional military ethic. At the core of the course is consideration of the work of several scholars who have attempted to develop a theory of civil-military relations, using such concepts as power, professionalism, and ideology to organize their theoretical approach. The various traditions in the history of the American approach to war are analyzed and evaluated: the Hamiltonian, the Jeffersonian, the Wilsonian, and the Jacksonian. Against this background, the course proceeds to analyze critically the American experience in and approach to war, using various case studies as the empirical data for testing the theories and determining which traditions best explain the American approach.

ID: 6960
Prerequisites: None
Competencies: Not Specified
Delivery Type: Instructor-Led

Level: Masters
Length: Semester
Cost (Type): Yes
Provider: NDU>CISA
Entry Date: 07/06/2011
Update: 03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

DYNAMICS OF TERRORISM

T/E168 - PDU 45

This course examines terrorism as a contextual phenomenon produced by the manner in which individuals, organizations, and the state are situated within larger surroundings. Case studies and use of primary documents are used to explore the multiple forms of and motives for terrorism. Students examine origins of terrorism in the splintering of social movements, followed by the strategic and operational choices faced by the splinter and its members. Works by key theorists are supplemented by in-depth examination of particular episodes of terror to emphasize that even agency (individual choice) is bounded by a host of social and personal factors and constraints.

ID: 6975

Prerequisites: None

Competencies: Not specified

Delivery Type: Instructor-Led

Level: Masters

Length: Semester

Cost (Type): Yes

Provider: NDU>CISA

Entry Date: 07/06/2011

Update: 03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

DYNAMICS OF COUNTERTERRORISM

T/E169 - PDU 45

This course provides an examination of the counterterrorism response at the national and international levels. Case studies and use of primary documents allow students to examine the implications for appropriate and comprehensive response. Students analyze strategic response by exploring the appropriate campaigns constructed to neutralize components of insurgent strategy. As a culminating exercise, students develop a national counterterrorism plan.

ID: 6976

Prerequisites: Not Specified

Competencies: Information Security, Classification Management, Personnel Security

Delivery Type: Web-Based Training

Level: Not Specified

Length: 2 Hours 30 Minutes

Cost (Type): Not Specified

Provider: NDU>CISA

Entry Date: 07/00/2011

Update: 03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

METHODS OF ANALYSIS & ARGUMENTATION

T/E170 - PDU 45

How well leaders, executives, managers, and other decision-makers analyze, evaluate, and argue over their options affects the quality of decisions and policies. Effective decision-makers use not only their direct knowledge but also their skill at estimating when they need help. Therefore, CISA 6942 provides an introductory overview of methods of analysis and argumentation to equip decision-makers to utilize methods from different sources and under varied conditions, and to help them pursue future additional study as needed. Focusing on modern complex security challenges such as terrorism, the course examines the application of these methods: their ideas, the tools they offer, and the situations that may evoke them, and options for their further study. The course frequently discusses the logic of arguments, the approach of different natural sciences, social sciences, mathematics, law, journalism, and politics. The course also examines similarities and differences between a written communication, such as a report, and a verbal communication, such as a briefing. Our goal is clarity, self-awareness, and a critical perspective on alternatives, developing arguments, presenting findings, and recommending actions. The course aims mainly at students with professional backgrounds and will utilize student experience for examples and problems. This course also enables students to start on their student research project.

ID: 6942

Prerequisites: None

Competencies: Information Security, Classification Management, Personnel Security

Delivery Type: Instructor-Led

Level: Masters
Length: Semester
Cost (Type): Yes
Provider: NDU>CISA
Entry Date: 07/06/2011
Update: 03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

T/E171 - PDU 45

This course examines the role military power has historically played in shaping cooperation, competition, and conflict among nation-states. It examines the interrelationship between military and nonmilitary instruments of power. Students will explore different models of the international system and basic tenets of strategic thought. After reviewing the structure of the U.S. national security decision-making process and America's post-World War II national strategy, the course will conclude with an examination of nuclear, conventional, and low-intensity conflict and strategy.

ID: 6902
Prerequisites: Not Specified
Competencies: Not Specified
Delivery Type: Instructor-Led

Level: Masters
Length: Semester
Cost (Type): Yes
Provider: NDU>CISA
Entry Date: 07/06/2011
Update: 03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

NATIONAL SECURITY DECISION MAKING

T/E172 - PDU 45

How are national security decisions made, especially in light of the need to anticipate future events, achieve goals, reduce surprise, and avoid disaster in the public as well as private sector? This course relates analytical tools to decision-making styles of organizations and individuals in different environments, especially competitive settings such as combat, international relations, and business. Students will examine complexity, nonlinearity and chaos theory, systems dynamics, and scenario construction.

ID: 6940
Prerequisites: Not Specified
Competencies: Program Security
Delivery Type: Instructor-Led

Level: Masters
Length: Semester
Cost (Type): Yes
Provider: NDU>CISA
Entry Date: 07/06/2011
Update: 03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

T/E173 - PDU 45

This course seeks to promote understanding of classic strategic thought and to prepare the student to think strategically in a fundamentally changed security environment. It examines the etiology of strategy and the foundations of modern strategy, relying on key strategic thinkers to examine the relationship between strategy and policy. Clausewitz argued that war has its own language (violence) but not its own logic (politics). Politics determines the aims for which war is fought and devises the strategy to achieve those aims. Lessons will be drawn from both historic and recent case studies, including the Peloponnesian War, the American Revolution, Vietnam, and Iraq. Students will examine whether the nature of war is changing, as the New War theorists argue, or whether its basic parameters remain. Students will examine post-9/11 strategic thought, including the strategy of non-state armed groups such as Al-Qaeda, to understand both the nature of war and of strategy in the post-9/11 security environment.

ID: 6901
Prerequisites: Not Specified
Competencies: Program Security
Delivery Type: Instructor-Led

Level: Masters
Length: Semester
Cost (Type): Yes
Provider: NDU>CISA
Entry Date: 07/06/2011
Update: 03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

PRINCIPLES OF POLITICAL WARFARE

T/E174 - PDU 45

A nation's political, economic, and military tools must serve a common purpose. It is widely recognized that our ability to win a war is dependent on winning politically as much as it is militarily. Despite this fact, America's ability to wage effective political warfare is, at best, underdeveloped. Our unwillingness to recognize that international political activity can and should be considered a form of warfare, as well as our own cultural and bureaucratic obstacles, make it extraordinarily difficult for the U.S. to conduct political warfare. This course will begin by reviewing the links between grand strategy and political warfare. It will then identify its various elements and examine how these various elements are used to achieve a country's strategic objectives. We will analyze several political warfare campaigns and determine the reasons for these campaigns' success or failure. Finally, we will propose ways to overcome existing obstacles to an effective political warfare capability.

ID: 6928
Prerequisites: Not Specified
Competencies: Not Specified
Delivery Type: Instructor-Led

Level: Not Specified
Length: 2 Hours
Cost (Type): Yes
Provider: NDU>CISA
Entry Date: 07/06/2011
Update: 03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

SCIENCE AND POLICY OF BIOTERRORISM AND BIOWAR

T/E175 - PDU 45

This course aims to provide students with an understanding of the living agents or organic products of potential use in warfare, terrorism, or criminal activities in the context of diplomatic and political implications of such weapons of mass destruction. Students will gain an appreciation of the scientific and political scope of biological agents and their potential for deployments against humans, animals, and plants. Information regarding clinical and scientific features or environmental issues of biological agents, toxins, or chemical agents is included. How to distinguish innocent from questionable use of dual-use, high-tech equipment will be discussed. The roles of various agencies including the Homeland Defense Department will be elucidated. Responsibility of the private sector, Federal, State, and local agencies and the military in homeland defense are examined. Solutions such as political, psychological, and physical deterrence, counterforce, active defense, and crisis and consequence management, etc., will be discussed.

ID: 6932
Prerequisites: Not Specified
Competencies: Not Specified
Delivery Type: Instructor-Led

Level: Masters
Length: Semester
Cost (Type): Yes
Provider: NDU>CISA
Entry Date: 07/06/2011
Update: 03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

T/E176 - PDU 45

This course addresses some of the essential questions that need to be addressed in a course on science, technology, and national security policy, such as the role of science and technology in the development of national security policy, the importance of politics in scientific and technological endeavors, the trade-off calculations decision makers must make when making the kind of "cardinal choices" associated with science, technology, and national security, the factors at work in the processes associated with scientific and technological innovation, and impact technology has had on the ability to win wars, for example in the case of the war with Iraq.

ID: 6934
Prerequisites: Not Specified
Competencies: Not Specified
Delivery Type: Instructor-Led

Level: Masters
Length: Semester
Cost (Type): Yes
Provider: NDU>CISA
Entry Date: 07/06/2011
Update: 03/28/2012

Link: http://www.dss.mil/seta/index.html

INTERNAL SECURITY STRATEGIES

T/E177 - PDU 30

What are the elements of an effective and efficient internal security strategy? How does a nation's internal security strategy differ from its overall national security strategy? Equally important, how does a nation go about solving the formidable problem of integrating its internal and external security strategies? Using several case studies, this course will examine how five nations have rewritten their internal security strategies in the post-9/11 era to deal with the threat posed by transnational terror organizations. In so doing, we will attempt to understand how each nation has gone about balancing civil rights and security, integrating law enforcement and intelligence, and resolving the competing interests of the political, diplomatic, military, judicial, and intelligence establishments. The objectives of the course will be to build a framework by which to, first, understand strategy building process and, second, assess the effectiveness of each nation's internal security strategy.

ID: 6988
Prerequisites: Not Specified
Competencies: Not Specified
Delivery Type: Instructor-Led

Level: Masters
Length: Semester
Cost (Type): Yes
Provider: NDU>CISA
Entry Date: 07/06/2011
Update: 03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

INTERNATIONAL LAW AND GLOBAL SECURITY

T/E178 - PDU 30

International Law and Global Security is designed to introduce students to the core principles and defining features of the international legal system, and to the changing role of international law in contemporary national and global security. Emphasis will be placed on the applicability of international law to armed conflict, counterterrorism, and containing the spread of weapons of mass destruction.

ID: 6982

Prerequisites: Not Specified

Competencies: Not Specified

Delivery Type: Instructor-Led

Level: Masters

Length: Semester

Cost (Type): Yes

Provider: NDU>CISA

Entry Date: 07/06/2011

Update: 03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

POLITICAL ISLAM: ORIGINS, THREATS AND COUNTERSTRATEGIES

T/E179 - PDU 30

The course gives an overview of political Islam, with an emphasis on radical political Islam. It provides an in-depth analysis of the ideological roots, structural causes, and organizational structures of radical political Islamic movements by examining various movements such as the Muslim Brotherhood, Hamas, Hezbollah, Al Qaeda, and Jamaat al-Islamiyya. Through a comparative analysis of these movements, the course lays out the commonalities in their rhetoric, the conditions under which they emerge and radicalize, and the types of threat they pose to democratic legal order. Drawing on these findings, the course offers counterstrategies against these threats.

ID: 6921
Prerequisites: Not Specified
Competencies: Not Specified
Delivery Type: Instructor-Led

Level: Masters
Length: Semester
Cost (Type): Yes
Provider: NDU>CISA
Entry Date: 07/06/2011
Update: 03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

GLOBALIZATION AND NATIONAL SECURITY

T/E180 - PDU 30

Globalization and National Security examines the phenomenon of globalization, its drivers, and its implications to national security in the 21st century. Globalization has revolutionized and accelerated the way goods, services, information, and ideas are sourced, produced, delivered, and circulated worldwide. Greater integration and interconnectivity have dramatically improved the quality of life for global citizens. However, all these benefits have been accompanied by increased risks that threaten not just the global economy but international security due to intense competition for labor, capital, technology, and natural resources around the world. This course analyzes the different socio-economic drivers of globalization and concludes with an evaluation of national and international strategies to address the national security challenges posed by globalization.

ID: 6945

Prerequisites: Not Specified

Competencies: Not Specified

Delivery Type: Instructor-Led

Level: Masters

Length: Semester

Cost (Type): Yes

Provider: NDU>CISA

Entry Date: 07/06/2011

Update: 03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

FOUNDATIONS FOR HOMELAND SECURITY

T/E181 - PDU 45

Foundations and Issues of Homeland Security frames the topic of homeland security. Topics include: Threat, Threat Definition and Assessment; Means and Methods for Securing the Homeland; Introduction to Organization and Coordination Issues; and Law, Legal Institutions, and Legal Constraints on Roles & Mission.

ID: 6950
Prerequisites: Not Specified
Competencies: Not Specified
Delivery Type: Instructor-Led

Level: Masters
Length: Semester
Cost (Type): Yes
Provider: NDU>CISA
Entry Date: 07/06/2011
Update: 03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

ORGANIZING HOMELAND DEFENSE

T/E182 - PDU 45

As the core course of the Homeland Defense Fellowship (HDF) program, Organizing for Homeland Defense provides the essential knowledge enabling our HD Fellows to navigate strategic changes, understand lessons learned and deduce the applicability or unique sui generis aspects of approaches deployed since September 11, 2001. The course addresses the foundations and core issues of Homeland Defense and Homeland Security. Students who complete Organizing for Homeland Defense must demonstrate the ability to: understand the dimensions of the contemporary security environment; assess the contemporary spectrum of conflict and how domestic national security architectures are challenged by new or renewed threats of an unconventional nature; evaluate the lessons learned from seminal case-studies which span the scale of homeland threats from natural to manmade; and understand the U.S. response to the new threat environment and how best to build international capacities and capabilities to meet common challenges in Homeland Defense.

ID: 6951

Prerequisites: Not Specified

Competencies: Not Specified

Delivery Type: Instructor-Led

Level: Masters

Length: Semester

Cost (Type): Yes

Provider: NDU>CISA

Entry Date: 07/06/2011

Update: 03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

STRATEGIC LEADERSHIP FOR HOMELAND SECURITY

T/E183 - PDU 45

This course prepares prospective senior leaders to think critically about strategic challenges in homeland defense and to employ best available tools to craft solutions. Students will develop strategies for linking national resources and capabilities with homeland defense objectives.

ID: 6953
Prerequisites: Not Specified
Competencies: Not Specified
Delivery Type: Instructor-Led

Level: Masters
Length: Semester
Cost (Type): Yes
Provider: NDU>CISA
Entry Date: 07/06/2011
Update: 03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

T/E184 - PDU 45

This course examines the growing national security threat posed by the relationship between terrorism and crime. The unprecedented pace of globalization and technological advance in the post-9/11 world has enhanced the effectiveness of terrorist groups and criminal organizations, allowing each to benefit from the strengths of the other. Drawing on a series of 40 case studies, Terrorism and Crime analyzes how terrorists and crime syndicates leverage criminal activities (e.g., drug trafficking, money laundering, arms trafficking, human smuggling, counterfeiting, and cyber crimes) to promote their mutual and respective interests. The course concludes with an evaluation of strategies that address these terrorist and transnational criminal threats at both the national and international level.

ID: 6978
Prerequisites: Not Specified
Competencies: Personnel Security
Delivery Type: Instructor-Led

Level: Not Specified
Length: Semester
Cost (Type): Yes
Provider: NDU>CISA
Entry Date: 07/06/2011
Update: 03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

T/E185 - PDU 45

This course will help the student explore the changes in the nature of conflict in the last decade of the 20th century and the implications for the 21st century by examining the boundaries of peace operations, the actors, the organizational structures, and the resources required to perform these extremely complex missions. This course will examine the roles of the United Nations, the United States, NATO, and nongovernmental organizations across the range of peace operations—from peacekeeping to peace enforcement and peacemaking to peace-building.

ID: 6953
Prerequisites: Not Specified
Competencies: Not Specified
Delivery Type: Instructor-Led

Level: Not specified
Length: Semester
Cost (Type): Yes
Provider: NDU>CISA
Entry Date: 07/06/2011
Update: 03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

U.S. FOREIGN POLICY

T/E186 - PDU 45

This course sets policy context for prosecution of war on terrorism, by placing current problems in the larger setting of persisting themes in U.S. foreign policy. It examines foreign policy challenges in critical regions, considers linkages between terrorist organizations around the globe, and relates U.S. responses to national interests, resources, domestic politics, ideology, and agencies. The course addresses the challenges of coalition-building and alliance cohesion, costs, risks of military interventions, and the problems of nation building and reconstruction.

ID:	6906	**Level:**	Not Specified
Prerequisites:	Not Specified	**Length:**	Semester
Competencies:	Personnel Security	**Cost (Type):**	Yes
Delivery Type:	Instructor-Led	**Provider:**	NDU>CISA
		Entry Date:	07/06/2011
		Update:	03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

JIHADIST GLOBAL STRATEGIES

T/E187 - PDU 45

This elective course examines current geopolitics with a particular focus on the surge, expansion and evolution of Salafi-Jihadi and Khomeinist-Jihadi movements. Students will be introduced to the evolution of strategic options during and after the Cold War and before and after September 11, 2001. Students will assess current strategies and analyze future options.

ID: 6922
Prerequisites: Not Specified
Competencies: Not Specified
Delivery Type: Instructor-Led

Level: Not specified
Length: Semester
Cost (Type): Yes
Provider: NDU>CISA
Entry Date: 07/06/2011
Update: 03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

WAR AND DEMOCRACY

T/E188 - PDU 30

This course will examine the nexus between war and democracy. It will begin by assessing the claims of democratic peace theory, the notion that democracies are inherently peaceful and that democracies are less likely to engage in war. It will also examine the post-Cold War correlate that democratization will improve the prospects for international peace, and it will examine whether the democratic peace thesis is applicable to domestic and civil wars. In the second part of the course, students will examine Thucydides' contention that protracted war made Athens less democratic. Democracies face a number of challenges during war, and we will assess these in terms of a few long wars, including the Second World War, Vietnam and the current War on Terror. Finally, students will examine the nexus between war termination and democracy. Why is it so difficult for democracies to manage expectations, realize the objectives of war, and bring war to a successful conclusion?

ID: 6927

Prerequisites: Not Specified

Competencies: Personnel Security

Delivery Type: Instructor-Led

Level: Masters

Length: Semester

Cost (Type): Yes

Provider: NDU>CISA

Entry Date: 07/06/2011

Update: 03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

MILITARY POWER AND THE INTERNATIONAL SYSTEM

T/E189 - PDU 30

This course begins with the development of the modern nation-state system and the different concepts of national, international, and global security. In addition, it offers insight into political, technological, social, and organizational factors transforming the military instrument of power. The major section focuses on the evolving role military power has historically played in shaping cooperation, competition, and conflict in the international system. Students will examine the interaction of political and military strategies of Great Powers shaping European/Western history over several subsequent epochs from the Middle Ages to the post-Cold War era. The course will conclude with a discussion of current international security policies and doctrines, possible future structures of the international system, and the transformation of war. This course prepares students to understand the evolution of the modern nation state system and the role that military force has played in shaping it.

ID: 6907

Prerequisites: Not Specified

Competencies: Not Specified

Delivery Type: Instructor-Led

Level: Not Specified

Length: Semester

Cost (Type): Yes

Provider: NDU>CISA

Entry Date: 07/06/2011

Update: 03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

STRATEGIC SCENARIOS FOR POST-INDUSTRIAL FUTURES

T/E190 - PDU 30

Our generation believes that it is "post-industrial" with unique, complex and surprising security problems. This course examines these claims and therefore is about strategic management for discontinuous, as opposed to smoothly evolving, change. We examine innovative methods of futures analysis, including scenario construction, and present some ideas for utilization and adaptation of ideas such as net assessment, Project Horizon, alternative history, wicked problems, opposed systems design, black swans, the innovator's dilemma, the art of the long view, sources of power, why smart executives fail, and the psychology of intelligence analysis.

ID: 6908
Prerequisites: Not Specified
Competencies: Personnel Security
Delivery Type: Instructor-Led

Level: Masters
Length: Semester
Cost (Type): Yes
Provider: NDU>CISA
Entry Date: 07/06/2011
Update: 03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

GOVERNANCE, GANGS AND GARRISON: SECURITY ISSUES IN LATIN AMERICA AND THE CARIBBEAN REGION

T/E191 - PDU 30

This course examines the coercive strategies and interactions of armed groups -- such as gangs, criminal syndicates, militias, terrorist bands, web hackers, and pirates -- with other actors and environments. It explores the policy implications as traditional social and political institutions deal with these violent entities. We further explore what happens when individuals and traditional communities, desiring stable rule of law, find themselves confronted with the consequences of anarchic, fragmented, and adaptive social arrangements. Cases from Latin America, the Caribbean region, and other countries and dimensions illustrate conceptual discussions and policy implications.

ID: 6915

Prerequisites: Not Specified

Competencies: Not Specified

Delivery Type: Instructor-Led

Level: Masters

Length: Semester

Cost (Type): Yes

Provider: NDU>CISA

Entry Date: 07/06/2011

Update: 03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

T/E192 - PDU 45

To gain a general understanding of the nature of special operations forces and of their modes of employment, this 2-credit elective course introduces the student to the essential history of U.S. special operations forces and their use. The student grapples with challenges of global terrorism and assessment of success.

ID: 6962
Prerequisites: Not Specified
Competencies: Personnel Security
Delivery Type: Instructor-Led

Level: Masters
Length: Semester
Cost (Type): Yes
Provider: NDU>CISA
Entry Date: 07/06/2011
Update: 03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

T/E193 - PDU 30

This elective course examines how to employ a "whole of government" approach to stabilization and reconstruction outcomes. This seminar adopts an ends, ways, and means analytical framework to determine better orchestrated interagency outcomes along 6 government lines of development, namely security; governance and participation; humanitarian assistance and social well-being; economic stabilization and infrastructure; and justice and reconciliation. Students will learn to work within volatile, uncertain, complex and ambiguous (VUCA) environments and will leave the course better able to think strategically about national security and the interagency process within an ever-changing global security environment across the full spectrum of conflict.

ID: 6962
Prerequisites: Not Specified
Competencies: Personnel Security
Delivery Type: Instructor-Led

Level: Masters
Length: Semester
Cost (Type): Yes
Provider: NDU>CISA
Entry Date: 07/06/2011
Update: 03/28/2012

Link: http://www.ndu.edu/cisa/academic_catalogue.cfm

SECURITY AWARENESS TRAINING VIA GS CONNECT

T/E194 - PDU ?

You will learn the importance of information security within your agency and understand the Federal regulations regarding information security. Work on the leading edge of information technology (IT) security by identifying potential security threats and protecting your organization's computer system.

* Online independent study course
* Four-week access to recorded lectures and content
* Weekly assignments
* Instructor support via e-mail

ID: SRTY7030A

Prerequisites: None

Competencies: Information Security, Information Assurance and Cyber Security

Delivery Type: Instructor-Led

Level: Not specified

Length: 4 weeks

Cost (Type): Yes

Provider: DOA > DOA Graduate School

Entry Date: 06/24/2011

Update: 03/28/2012

Link: http://www.graduateschool.edu/course_details.php?cid=SRTY7030A

CERTIFIED INFORMATION SYSTEM SECURITY PROFESSIONAL (CISSP) PREP

T/E195 - PDU 30

CISSP designation has clearly emerged as the pivotal certification in the security field. This 5-day prep course provides entry-level professionals the broad skill set needed to protect against and defeat hackers. Increase your knowledge of various types of intrusion detection techniques and countermeasures used in building secure, impregnable networks. Then get hands-on training in labs designed to simulate what your organization will encounter in the real world and reinforce the skills discussed throughout the class. This course is essential to get the intensive training needed in preparation for the CISSP certification exam.

ID: SRTY9100T

Prerequisites: None

Competencies: Information Assurance and Cyber Security, Incident Response

Delivery Type: Instructor-Led

Level: Not Specified

Length: 5 days

Cost (Type): Yes

Provider: DOA>DOA Graduate School

Entry Date: 06/24/2011

Update: 03/28/2012

Link: http://www.graduateschool.edu/course_details.php?cid=SRTY9100T

BUDGETING AND FINANCIAL MANAGEMENT FOR SECURITY PROGRAMS

T/E223 - PDU 45

This course provides an integrative study of financial management through applied security problems and case studies. Topics reflect the changing environment of financial management and include decision-making; the role of intangibles in value creation; financial performance metrics; strategic financial planning and control; strategic valuation decisions; growth strategies for increasing value; the restructuring of financial processes; DoD governance and financial ethics; value-based management; strategic cost management; and the impact of information technology on financial systems.

ID: ED505.01

Prerequisites: None

Competencies: Continuity of Operations Planning, Security Program Management

Delivery Type: Web-Based

Level: Not Specified

Length: 16 Weeks

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 08/29/2012

Update:

Link: http://www.dss.mil/cdse/catalog/elearning/ED505.html

HUMAN RESOURCE MANAGEMENT FOR DOD SECURITY

T/E224 - PDU 45

This course will provide an educational opportunity for mid-career security specialists to gain in-depth knowledge and understanding of human resource management (HRM) to support DoD security programs. The course shall address how senior security leaders make human capital decisions. It explores the skills and tools needed to make effective HRM decisions in DoD security. The course also examines how security policy and programs impact HRM throughout DoD and the defense industrial base.
This course will develop each student's ability to use this knowledge to become more effective as a security leader in the DoD. This course includes reading, research, and writing assignments similar to a three credit-hour college or graduate-level course.

ID: ED506.01

Prerequisites: None

Competencies: Continuity of Operations Planning, Security Program Management, Personnel Security

Delivery Type: Web-Based

Level: Intermediate

Length: 16 Weeks

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 08/29/2012

Update:

Link: http://www.dss.mil/cdse/catalog/elearning/ED506.html

RESEARCH METHODS, STATISTICS, AND REPORTING TO SUPPORT DOD SECURITY PROGRAMS

T/E225 - PDU 45

This course will help prepare the senior security manager to demonstrate clarity in the strategic interpretation of empirical vs. notional-based recommendations in order to justify resources, critically evaluate feasibility of research proposals, and demonstrate program performance.
This course addresses research strategy and design, data collection, statistical and interpretive analysis, and final report preparation. The focus of this course is not on mastery of statistics but on the ability to use research in DoD Security environment.
This course will develop each student's ability to use this knowledge to become more effective as a security leader in the DoD. This course includes reading, research, and writing assignments similar to a three credit-hour college or graduate-level course.

ID: ED508.01

Prerequisites: None

Competencies: Security Tools and Methods, Security Program Management

Delivery Type: Web-Based

Level: Advanced

Length: 16 Weeks

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 08/29/2012

Update:

Link: http://www.dss.mil/cdse/catalog/elearning/ED508.html

ASSESSMENT AND EVALUATION OF DOD SECURITY PROGRAMS

T/E226 - PDU 45

This course covers the ways in which security managers can establish and share concrete achievements or measurements (metrics) that effectively demonstrate the impact of security programs and activities.
This course will enable students to examine and summarize methods used for assessing and evaluating security programs across DoD; strategize how to integrate effective assessments and evaluations into security programs for mission assurance; assess the impacts of policies and plans on assessments and evaluations on security programs; examine the impact of assessments and evaluations from higher-echelon and installation-level perspectives; analyze and validate collected data and metrics from assessments and evaluations to effectively justify expenditures for security program requirements; assess and analyze the costs and effects of assessments and evaluations to establish an effective business case; examine approaches to successfully communicate the outcomes of assessments and evaluations in a persuasive manner; and assess the effectiveness of new and existing security policies and procedures.
This course will develop each student's ability to use this knowledge to become more effective as a security leader in the DoD. This course includes reading, research, and writing assignments similar to a three credit-hour college or graduate-level course.

ID: ED509

Prerequisites: None

Competencies: Security Tools and Methods, Security Program Management

Delivery Type: Web-Based

Level: Not Specified

Length: 16 Weeks

Cost (Type): No

Provider: DoD>DSS>CDSE

Entry Date: 08/29/2012

Update:

Link: http://www.dss.mil/cdse/catalog/elearning/ED509.html

THE FUTURE OF SECURITY SYSTEMS AND INFORMATION ASSURANCE

T/E227 - PDU 45

This course is designed for the senior security manager of the 21st century. It addresses leading-edge technologies and their implications (positive and negative) for the field of security within DoD. It is designed to help security personnel thrive in an information systems environment.

The course will prepare students to describe the current security environment, including the risks and opportunities that are inherent in new processes and technologies; summarize the nature and role of information; evaluate the essential issues involved in sharing and protecting information, including issues of risk, knowledge sharing, and education; describe the interrelationships among elements that comprise a modern security system, including hardware, software, policies, and people; recognize and distinguish the functions and types of modern security systems and illustrate them using specific examples; identify and assess the trade-offs that system developers should consider when designing, implementing, and operating balanced security systems; explain the factors and issues that frame the possible future security environments, and estimate the effect of these issues on current security design and operations; discuss and evaluate the effectiveness of how information assurance principles are applied in the DoD Information Assurance Certification and Accreditation Process (DIACAP); discuss and evaluate the effectiveness of how information assurance principles are applied in the National Industrial Security Program; discuss and evaluate the strengths, limitations, and vulnerabilities of information systems that currently exist to support DoD Security Programs that could or should be developed in the future (near-term and long-term) to support DoD security.

This course will develop each student's ability to use this knowledge to become more effective as a security leader in the DoD. This course includes reading, research, and writing assignments similar to a three credit-hour college or graduate-level graduate-level course.

ID: ED510

Prerequisites:

Competencies: Information Assurance/ Cyber Security

Delivery Type: Web-Based

Level: Advanced

Length: 16 Weeks

Cost (Type): No

Provider: DoD > DSS > CDSE

Entry Date: 08/29/2012

Update:

Link: http://www.dss.mil/cdse/catalog/elearning/ED510.html