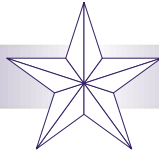


# 2012 Course Catalog





***The National Security Training Institute is dedicated to the advancement of the security professional through the presentation of courses and seminars in the national security arena.***

***NSTI is known for highly interactive training provided by nationally recognized security experts from all the security disciplines. The courses and seminars meet the needs of the career security professional – entry level, journeyman and expert.***

It is my pleasure to present the 2012 National Security Training Institute Course Catalog. The courses outlined in this catalog represent a significant collective investment in curriculum development. Each course is designed with one overarching objective—the development of a multidiscipline security officer. It is my hope you will visit us at one of our courses this year. I guarantee that it will be the best investment you have made in your professional development in 2012!

deedee collins  
Executive Director

### ***What Sets Us Apart!***

---

At NSTI our courses are known for being the best in “hands-on” and interactive training. Every student leaves feeling they have learned something they can apply on the job. Features of NSTI training include:

- **Small Class Sizes** (on average 16-20 per class)
- **Highly Interactive Training** (daily exercises, team projects, prizes!)
- **A Network of People** ( the instructors are the best in the profession and you meet students from across the intelligence community)
- **Resources To Help You On the Job** (every student leaves with a full library of security documentation in softcopy)

### ***Training Where You Want It!***

---

Are you interested in hosting a class in your area? NSTi offers the chance to hold any of our courses at your facility. The three requirements for holding a training event at your location:

1. Meet the minimum number of students.
2. Allow us to add students from the surrounding area.
3. Provide an adequate training facility.

**For more information, contact NSTI’s Registrar, Teresa Lawrence at 703-263-9113 or [tlawrence@nstii.com](mailto:tlawrence@nstii.com)**





## **Analytical Risk Management (ARM)**

**Course Director:** Dan See

### **Course Description**

Security organizations today are faced with the challenge of addressing evolving threats, while utilizing limited resources. These threats come from a variety of sources: physical, technical, natural, or accidental, to name a few. The days of unlimited security budgets are over and the security community needs a structured approach to prioritize risk mitigation strategies, using cost/benefit analysis. The Analytical Risk Management process provides security professionals with the necessary tools to identify and prioritize risks, and to manage those risks. Attendees develop the knowledge to fully understand and implement risk management fundamentals in the establishment of a risk management program. During this course we discuss risk assessment, risk reporting, and other risk management methodologies and publications such as the NIST 800-37 Rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems* and the *National Infrastructure Protection Plan*, Chapter 6 on Risk Management.

### **Target Audience**

Personnel who provide risk assessments and mitigation recommendations to senior managers responsible for accepting risk and funding of security programs.

### **Why Take the Course**

- Learn the national security policy required to employ the risk management methodologies.
- Be able to perform ARM cost/benefit analyses.

### **2012 Schedule**

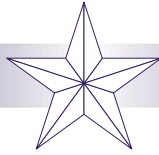
March 5 - 8, 2012

Chantilly, VA

October 9 - 12, 2012

Chantilly, VA





## Counterintelligence (CI)

**Course Director:** Rusty Capps

### Course Description

As the world's most active and persistent espionage perpetrators, China and Russia currently pose the greatest foreign threat to U.S. economic health and industrial competitiveness. Both view themselves as strategic competitors of the U.S. They have directed their intelligence services and industries to acquire economic and technical intelligence, sensitive manufacturing processes, trade secrets and dual-use technologies from developed countries, especially the U.S. Some specialists state that the scope and scale of this activity has surpassed that at the height of the Cold War.

In the CI course we review the structure, operational tradecraft and targeting activities of the Chinese Ministry of State Security (MSS) and People's Liberation Army (PLA) Department, as well as the Russian Foreign Intelligence Service (SVR) and Foreign Military Intelligence Directorate (GRU). Case studies illustrate the range and complexity of the threat, from "insider spies" to classic espionage and the accelerating onslaught of intrusions in the cyber domain. We detail the craft and practice of counterintelligence (CI); the hard won CI lessons of the Cold War and their application to the current situation; and the development of CI and security programs to protect corporate assets and competitiveness.

### Target Audience

Security professionals wanting to gain CI best-practices from experts with first-hand experience.

### Why Take the Course

- Apply the current espionage threat profile in aligning or developing protective counterintelligence and security programs to protect company assets and intellectual property.
- Gain a more robust comprehension of the CI environment and how it applies to security compromises.

### 2012 Schedule

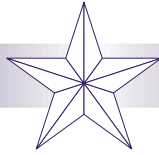
April 24 - 26, 2012

Chantilly, VA

November 27 - 29, 2012

Chantilly, VA





## Counterterrorism (CT)

**Course Director:** Daniel Mulvenna

### **Course Description**

Gain a tactical understanding of domestic and international terrorist attacks, including “lone wolves,” organized groups, and insurgent movements. This course provides knowledge of the terrorists’ mindsets and their tactics, techniques and procedures (TTP). Studying TTP enables the development and deployment of appropriate countermeasures to deter, detect and disrupt the terrorist attack cycle. Every terrorist attack is preceded by a variety of pre-incident indicators, specifically information and intelligence collection by the terrorists. Recognition of these pre-attack indicators provides opportunities to avoid potential attacks through appropriate reactive countermeasures. Understanding their requirements and behavior patterns can provide a critical edge to potential targets. Using decades of research on various movements and a wide variety of lessons-learned from actual terrorist attacks, this course provides participants with a CT knowledge base and skill-set that assists them in developing security awareness and protection programs for company personnel and assets.

### **Target Audience**

The security professional wanting to gain knowledge from CT experts with first-hand experience.

### **Why Take the Course**

- Raising awareness of the threat of terrorism assists participants in aligning or developing proactive and reactive awareness and protective programs in order to protect company personnel and assets.
- Develop and deploy CT safeguard countermeasures.

### **2012 Schedule**

February 28 - March 1, 2012

Chantilly, VA

September 11 - 13, 2012

Chantilly, VA





## Cybersecurity (CS)

**Course Director:** Paul Woodie

### Course Description

The hands-on Cybersecurity (CS) course delivers information on identity theft, viruses, malware, and cyber intrusions relating to our critical infrastructures like the power grid, and financial systems. These incidents are increasingly common and can have devastating personal and national security consequences. The course addresses various threats to computer systems and networks, and explains their implications on both an individual and national level. It also covers the growing body of laws, regulations, directives, and guidelines that influence both our personal, organizational, and national response to this significant threat. Through lecture, classroom discussion, computer demonstrations and exercises, students see examples of how to deal with threats using the three types of countermeasures defined by the National Institute of Standards and Technology (NIST): **Management** (what organizational steps can address this problem most effectively?), **Operational** (how can we respond to day-to-day computer incidents?) and **Technical** (how do we configure our computer and network systems for maximum resistance to these problems?). Each student is assigned a computer and applies newly learned skills via classroom exercises. Exercises include testing password strength, identifying network vulnerabilities, sniffing/eavesdropping to compromise information and recovering valuable information and evidence through digital forensics. Students return to their own work environment ready to implement their new knowledge.

The course includes tools used in class which the students take with them to enhance the cybersecurity posture of their own unique computer and network environment. An essential take-away resource list helps to expand knowledge, skills, and abilities in the important field of cybersecurity even after the course is finished.

### Target Audience

The course benefits those who have management responsibility for the security of their computers and networks. This course is a must for job titles such as FSO, CSSO, ISSM, security manager, however, all computer-users benefit from this instruction.

### Why Take the Course

- Gain a greater awareness of the increasing cyber threat to our computing environments. Awareness is the first step in improving your computer security posture.
- Acquire tools and training that will allow you to test the strength of your own computer security countermeasures through hands-on exercises in class.
- Analyze the security risks in your own unique environment so that you can use your limited security budget in the most effective manner possible.

### 2012 Schedule

May 1 - 3, 2012

December 4 - 6, 2012

Annapolis, MD

Chantilly, VA





## Excellence in Security Management (ESM)

**Course Director:** deedee collins

### **Faculty**

Dr. John Bordeaux  
Rusty Capps  
Robby Ann Carter  
Jeffrey Dodson  
Dr. Ray Falcione  
Michael Frazier  
Karl Glasbrenner  
... and others!

Bob Gleeson  
Mathew Hollandsworth  
Vince Jarvie  
Bill Kotapish  
Jim Linn  
Ray Musser  
Rob Rogalski

### **Course Description**

Excellence in Security Management (ESM) is essential for all mid-level security professionals moving toward upper management positions. This career-building experience prepares attendees to understand what it takes to become a senior leader through interaction with prominent leaders on issues affecting intelligence, defense and the industrial communities. Attendees are exposed to the best practices in the security industry in a setting that affords great personal interaction, learning and networking. One-on-one coaching is available for those desiring time with a facilitator during the seminar. Each day has a primary focus discussing principles in managing complex and integrated security programs.

### **Target Audience**

Mid- to senior-level security managers.

### **Why Take the Course**

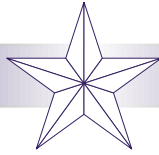
- Gain new expertise and tools to be successful in the security profession.
- Learn from the best minds in the security business and participate in hands-on application of management best practices.
- Take your career to the next level and become a leader in your organization.

### **2012 Schedule**

April 29 - May 3, 2012

Kent Island, Maryland





## Facility Security Officer Course (FSOC)

**Course Directors:** Jim Linn and Bill Laulo

### **Faculty**

Daniel Breazeal  
deedee collins  
Joe Cooper  
Lee Engle  
Michael Frazier  
Glenn Gates

George Hall  
Susan Jones  
Mitch Lawrence  
Gary Llewellyn  
Paul Woodie

### **Course Description**

This basic-level course is designed for individuals who have been designated as either the Facility Security Officer (FSO) or the Assistant FSO, and for the professional development of key security staff members responsible for the collateral aspects of the National Industrial Security Program (NISP). The FSOC familiarizes students with the requirements and practical application of the National Industrial Security Program Operating Manual (NISPOM). Mini-workshops, daily assessments on learning, and a final exam serve as the capstone of the course. This course greatly enhances preparations for the STEPP certification on-line examinations.

### **Target Audience**

FSO's and AFSSO's, CSSO's, CPSO's and security staff requiring comprehension of baseline NISPOM requirements.

### **Why Take the Course**

- Learn from instructors who have industrial security experience.
- Exposure to additional presenters with vast experience as security practitioners enhances classroom instruction.
- Build on your security toolkit with a comprehensive understanding of the NISP, an extensive collection of resources, references and job aids, and numerous networking points of contact.
- Gain preparatory training for the CDSE FSO Program Management Curriculum Exams leading to the DSS FSO Certification.

### **2012 Schedule**

March 5 - 9, 2012

Chantilly, VA

May 14 - 18, 2012

Chantilly, VA

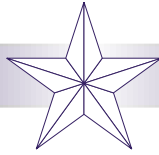
August 13 - 17, 2012

Chantilly, VA

November 5 - 9, 2012

Chantilly, VA





## ICD 503 Systems Security Practitioners Course (SSPC)

**Course Directors:** Greg Burch and Andrew Erne

### Course Description

The ICD 503 Systems Security Practitioners Course (SSPC) provides Information Assurance (IA) and Information System Security Managers (ISSMs), Information Systems Security Engineers (ISSEs), and Information Systems Security Officers (ISSOs) with skills to accomplish or oversee the implementation of Intelligence Community Directive (ICD) 503, and Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation. Students gain insights into the Federal Government's Certification & Accreditation transformation by examining the concepts of commonality, reuse and risk management from an enterprise perspective. Students learn the Risk Management Framework (RMF) and gain a comprehension of the key RMF roles and responsibilities. Instruction also includes categorizing information and information systems; security control families; common, hybrid, and system-specific security controls; tailoring and the identification of control enhancements; considerations for implementing security controls in the System Development Life- Cycle (SDLC); resources and references to assess and test security controls; the Body of Evidence to achieve authorization (accreditation); and considerations for continuous monitoring. The course provides a detailed walk-through of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 and NIST SP 800-53; and the Committee for National Security Systems (CNSS) Instruction 1253. Because most security professionals still encounter Director of Central Intelligence (DCID) 6/3 in the workplace as organizations gradually transition to ICD 503, this course provides a high-level overview of the DCID and highlights the most distinct differences between it and ICD 503.

### Target Audience

IT security personnel who are responsible for system certification and accreditation.

### Why Take the Course

- Gain a thorough understanding of the new national policy relative to systems certification and accreditation.
- Explore new concepts and approaches to using newly established and existing policy from across various components of the US government.

### 2012 Schedule

April 23 - 26, 2012

Chantilly, VA

July 16 - 19, 2012

Chantilly, VA

October 29 - November 1, 2012

Chantilly, VA





## Practical SCIF Construction (PSC)

**Course Director:** Joe Cooper

### Faculty

Bob Tschudi

Bruce Pomerleau

### Course Description

The Practical SCIF Construction (PSC) course is the premier physical security course offered to federal enterprise Special/Program Security Officers, facility engineers and space planners responsible for Sensitive Compartmented Information Facility (SCIF) planning, design and/or construction. This highly interactive course, offers practical instruction on how to build a SCIF. The course is based on the newly issued Director of National Intelligence (DNI) Intelligence Community Directive (ICD) 705 and Intelligence Community Standards 705-1 and 705-2. The course concentrates on SCIF design and construction standards, the accreditation process, and preparing a fully compliant Fixed Facility Checklist while reducing costs.

### Target Audience

Personnel involved in the management and/or design of SCIFs under ICD 705.

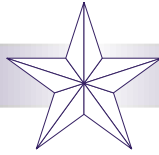
### Why Take the Course

- Understand ICD 705 requirements necessary to design a facility for a successful accreditation.
- Learn practical knowledge on design and construction techniques as well as material selection to meet the ICD requirements in the most cost effective manner.
- Interact effectively with architects, engineers, general contractors and facility personnel in the planning and construction phases, as well as provide knowledgeable security oversight during the lifecycle of the project.
- Enable security personnel to effectively advise their commanders or managers on the security requirements for SCIF construction projects.

### 2012 Schedule

March 19 - 23, 2012	Chantilly, VA
April 30 - May 4, 2012	Lexington, MA
June 25 - 29, 2012	Chantilly, VA
August 6 - 10, 2012	Chantilly, VA
October 1 - 5, 2012	Chantilly, VA
December 10 - 14, 2012	Chantilly, VA





## Program Security Management (PSM) Course

**Course Director:** Art Davis

### **Faculty**

Phil Bess

Robby Ann Carter

deedee collins

Joe Cooper

Honorable Martin Faga

Roy Gibson

Gary Harris

Mitch Lawrence

Jim Linn

Daniel Mulvenna

Mark Poirier

### **Course Description**

The Program Security Management (PSM) course is focused on mid-level security professionals with four to eight years of experience, who have been selected to advance but need more knowledge and specialized training than they can get in on the job training. The course focuses on methods that allow students to increase their productivity and value to their companies and the programs they administer and protect. The course employs presentations, interactive discussion and group case studies designed to challenge students to apply what they've learned. Students develop security plans, protection strategies and architectures for complex government programs based on real life scenarios.

### **Target Audience**

Mid-level security professionals.

### **Why Take the Course**

- Learn the latest in National Policy changes affecting you and your company and understand their real impact.
- Explore the business cycle within your company and how you (and security overall) can better support and add value to it.
- Hear experts explain the real value that security can provide to every aspect of the corporate environment.

### **2012 Schedule**

March 19 - 22, 2012

Chantilly, VA

October 29 - November 1, 2012

Chantilly, VA





## Security Awareness, Training and Education (SATE)

**Course Director:** Sue Jones

### Course Description

Who said security education couldn't be fun? A more positive approach to workforce compliance results in a more robust security program. In three hours, the SATE brief provides a variety of techniques to deliver a security education program that will be well received by your workforce and acceptable to your management. Let us help you put the "fun" in your fundamental role in helping your workforce understand and comply with security policy, procedures, requirements, warnings and prohibitions.

### Target Audience

Security personnel wanting to get fresh ideas on SATE program development.

### Why Take the Course

- Learn diversified methods to obtain compliance of security requirements and procedures from your workforce.
- Provide concepts of communicating security requirements from the perspective of marketing strategies.
- Discover economical methods that require no funding to support.

### 2012 Schedule

February 22, 2012

Chantilly, VA

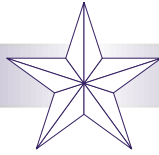
April 27, 2012

Chantilly, VA

June 6, 2012

Chantilly, VA





## Security Presentation Skills Seminar (SPSS)

**Course Directors:** deedee collins & Bill Kotapish

### **Course Description**

Edmund Burke once said, *“Education is the cheapest defense of a nation.”* To educate, you must be an effective communicator; a skill vital to success in the security profession. Each student gives four presentations in front of the class, two of which are video-taped for one-on-one sessions with an instructor. As part of the presentations and classroom discussions, students address their specific worksite security issues with the instructors for specific advice and guidance.

### **Target Audience**

Any security professional seeking to improve their communication skills.

### **Why Take the Course**

- Improve security communication skills.
- Learn to frame your message effectively and to sell your security program.
- Study proven best-practices to enhance your security awareness message.

### **2012 Schedule**

March 13 - 15, 2012

Chantilly, VA

October 9 - 11, 2012

Chantilly, VA





## Special Security Officer Course (SSOC)

**Course Director:** Bob Tschudi

### **Faculty**

Bruce Pomerleau

Sue Jones

Mathew Hollandsworth

Joe Cooper

Daniel Mulvenna

Susan Jennings

### **Course Description**

The Special Security Officer Course (SSOC) is designed for security professionals who administer all aspects of Sensitive Compartmented Information (SCI) programs. The SSOC familiarizes students with all Director of National Intelligence (DNI) Intelligence Community Directives (ICDs), Policy Memorandums and Policy Guidance. The course contains practical implementation exercises to give hands-on experience.

### **Target Audience**

Security personnel responsible for managing SCI programs.

### **Why Take the Course**

- Gain knowledge of laws, executive orders and regulations that govern IC security requirements.
- Enhance knowledge of the basic security disciplines and best practices that support the establishment and maintenance of an SCI security program.

### **2012 Schedule**

January 30 - February 3, 2012

April 09 - 13, 2012

July 23 - 27, 2012

September 10 - 14, 2012

December 17 - 21, 2012

Chantilly, VA

Chantilly, VA

Chantilly, VA

Chantilly, VA

Chantilly, VA

