

National Security Institute's 26th Annual Security Forum

# IMPACT 2011




National  
Security  
Institute

April 4 – 6, 2011  
Westfields Marriott, Chantilly, VA

## PROTECTING SECRETS: CONFRONTING A NEW WORLD OF RISK

### New for 2011...

- ★ Techniques to Counter Emerging Threats
- ★ NISP Compliance Strategies & Best Practices
- ★ Hands-on JPAS, AIS, ODAF Training
- ★ Security Lessons Learned & Case Studies
- ★ Innovative Ways to Improve Your Program



*"This was my first Impact conference and it really provides outstanding information combined with excellent networking opportunities."*

James E. Rylander  
CyberPoint International, LLC

*"Very interesting topics and great speakers. I am very impressed with the venue and the quality of all aspects of the conference. First class. Well worth the expense."*

Brandy Plotner  
Navy Fighter Weapons School



# BE INFORMED BE AWARE BE PREPARED

## Protecting Secrets: Confronting a New World of Risk

When it comes to the protection of classified and sensitive information, today's security professional requires more knowledge, and more understanding than ever before.

The to-do list for government and industry security professionals continues to grow, from coping with tighter budgets to navigating a growing array of threats. In today's changing security landscape, staying current is crucial to avoid serious compromise of classified information.

What's ahead? Which challenges are waiting to blindside you if you're not prepared?

**Find out at NSI IMPACT '11**, the premier event for security professionals. From the nuts and bolts of DoD Security, NISPOM and operations security to the biggest information security threats, you'll find the answers you need to do your job. With another outstanding agenda of the latest issues and innovative solutions, the IMPACT conference offers you exposure to top security experts in over 21 information-packed sessions delivering practical information you can't afford to miss.

## Hone Your Survival Skills

It's a pivotal moment in national security as global adversaries ramp up cyber attacks and continue their relentless pursuit of U.S. defense and technology secrets. You and your security program must evolve to meet the changing threat environment.

The new year brings dangerous new threats. Now is not the time to skimp on security, or security training as government and corporate secrets are even more vulnerable. IMPACT '11 will prepare you with proactive, effective and comprehensive security strategies essential to the success of your organization.

## Learn the "How-to" at IMPACT

Join the best minds in government and industry security for three innovative days at NSI's 26th Annual IMPACT '11 Conference and Expo on April 4-6 at the Westfields Marriott in Chantilly, VA.

Expert presentations, group discussions, case studies, and practical workshops look beyond the surface, giving you real and proven solutions that will work in your organization and prepare you for the security challenges ahead.

Whether you're new to the profession or an industry veteran, there's no better training opportunity than IMPACT to equip you with skills and resources you need to succeed.



## Informative Sessions, Practical Workshops and Solutions

Got questions about the National Industrial Security Program, the Joint Personnel Security Adjudication System, Security Clearance Automation, OPSEC, ODAA, SPPs and Automated Information Systems Security? Get answers at NSI IMPACT '11.

Learn everything you need-to-know from over 25 leading government and industry security experts at IMPACT '11 — the one conference your organization should attend this year.

### FREE BONUS WORKSHOP:

Pre-Conference JPAS Training  
Sunday, April 3, 2:00 pm – 5:00 pm

Open to conference attendees only, this three-hour bonus workshop delivers proven tactics and techniques to help you master the JPAS system. This hands-on training session will show you the ins and outs of JPAS, JCAVS and eQIP. Participants will have the opportunity to build skills and develop an enhanced working knowledge of the system.

## Your once-a-year opportunity to recharge, refocus and Re-energize

Why does the security community look forward to NSI IMPACT so eagerly every year?

**Agenda.** The agenda is targeted to your needs. IMPACT 2011 is programmed by security professionals who know the responsibilities of your job and the kind of pressures you face. They organize the schedule to make effective use of your valuable — and limited — time by focusing on the issues you face both day-to-day and long-term.

**Focus.** The participants are your peers. IMPACT 2011 draws its audience exclusively from government and industry security managers and professionals — the people who are doing the same job you're doing... the people you want to meet and share with.

**Environment.** Why get lost in a giant convention center or wait in long lines after a session to meet the speaker? IMPACT 2011 offers small, more intimate sessions that bring you closer to the experts and the speakers as well as your peers.

*"I think this seminar was extremely useful and I have gained a tremendous amount of knowledge. I will not miss this training!"*

*Lori, Barsanti, CACI International*

# IMPACT 2011 EXTRAS!

## 6 Reasons to Attend

### 1. Top speakers

Every speaker at IMPACT 2011 is renowned for the topic they will address. Expert instructors from government and industry will arm you with the skills and solutions necessary to successfully implement changing NISP requirements.

### 2. Targeted Topics

Participate in top-notch education. IMPACT 2011 is packed with sessions and workshops targeted to your specific needs so your time is always spent productively.

### 3. It's What You Asked for

We extensively surveyed hundreds of top security professionals to deliver the exact solutions to the most important challenges you face right now... and well into 2011.

### 4. Come away with Solutions

No other conference reveals proven tactics to guarantee enhanced security solutions you can take back with you and implement. You'll get the right balance between government and industry security issues, sessions for beginners through veteran security practitioners.

### 5. Practical, In-Depth Workshops

Interactive workshops provide extended training in critical security areas like JPAS; AIS security; counterintelligence awareness; international security; OPSEC; physical security; vulnerability assessment; security case studies, and valued lessons learned.

### 6. Professional Development

You'll get career-building strategies and a personalized road map for your professional growth while participating in sessions that you need to advance to the next level.

## Security Awareness Fair and Expo

Your registration includes admission to NSI's 2011 Security Awareness Fair and Expo. The major government security agencies will be there offering a broad array of complementary materials and media through their security outreach programs. These complimentary resources are ready to take back home with you to implement at your company or agency.

NSI's exclusive vendor expo brings you up-close to the hottest technologies, and products designed to help you handle ever-changing security challenges.

## A sampling of the 2011 Exhibitors



## Valuable Take-Home Resources

Every IMPACT 2011 registrant goes home with a comprehensive binder of conference materials and handouts and a DVD containing the 2011 Edition of NSI's Reference Library.



This remarkable DVD is packed with articles, white papers, checklists, glos-

saries, reports, statutes, executive orders, manuals, surveys, and primary sources. It is the most comprehensive collection of security-related information available, and it's all organized in a user-friendly format in categories that are meaningful to security professionals. If you ever need to write policies, prepare reports, plan strategy, forecast trends, or justify procedures... you'll appreciate having all this information at your fingertips.

We also will update you after the conference by e-mail with additional session handouts and presentations as they become available.

## Champagne Reception

**MONDAY, APRIL 4, 5:00-6:00PM**

Please join us for complimentary hors d'oeuvres and champagne. On Monday come meet your colleagues in a fun and relaxed setting, making contacts that will enhance your conference experience — and extend beyond.



**Monday  
April 4**

# EDUCATIONAL SESSIONS

## Keynote Address:



### Defending Against Cyber Threats in Dangerous Times

*General Michael V. Hayden  
Principal, Chertoff Group, Former  
Director CIA, NSA*

Few know more intimately how the global threat matrix and challenge of security has changed in the 21st century than General Michael V. Hayden. As former director of the National Security Agency and the Central Intelligence Agency, he understands the dangers, risks, and cyber threats facing America today. Now a principal with the Chertoff Group — a security consultancy co-founded by former Homeland Security Secretary Michael Chertoff — Gen. Hayden has unmatched insight into the security problems faced both by America's governmental institutions and it's largest and most critical businesses. In this eye-opening keynote address Gen. Hayden will outline the threats that most occupy the minds and budgets of government and defense industry security professionals. He will examine what's driving today's emerging cyberthreat landscape and what can we expect to see during 2011.

Monday, April 4 8:45am-9:40am

### Russian Espionage: The Bear is Back

*Oleg Kalugin, Former KGB Major  
General, CI Centre Professor*

The uncovering of a Russian spy ring in the U.S. demonstrates that while the Cold War may have thawed, international espionage continues to thrive. In a plot right out of a spy novel, the agents lived for more than a decade in American cities and suburbs where they seemed to be ordinary couples working ordinary jobs. Experts on Russian intelligence expressed astonishment at the scale, longevity, and dedication of the "sleeper" program. The Bear is indeed back without the restraints of the Cold War and it's easier than ever for Russian intelligence officers to meet, develop and recruit Americans. None of this is a surprise for KGB veteran Major General Oleg Kalugin who will share his insights into today's Russia, the resurgence of the KGB and how Russia is targeting our nation's most valuable secrets.

#### You Will Learn:

- Scope of Russian spying activities in the U.S.
- Recent spy cases and lessons learned
- How organizations are currently being targeted

Monday, April 4 10:40am-11:25am

### The Insider Threat: Confronting A New World of Risk

*Ira Winkler, President  
Internet Security Advisors Group*

Recent security breaches bring an emerging trend into focus—outsiders gaining insider privileges so they can access sensitive data. Trusted insiders also present a potentially significant threat, particularly when their access rights to classified information are inadequately controlled. As security is being tightened in the aftermath of the Wikileaks scandal, federal agencies and contractors are being asked to look within the perimeter and assess the ever-present insider threat. Ira Winkler, noted security expert and author of "Spies Among Us," will examine the biggest insider threats and best practices for preventing them. He will describe how easy it is for outsiders to become trusted insiders as he draws on his experience with recent headline security breaches and his involvement in the WikiLeaks investigation. He will also recommend countermeasures for securing your critical data.

#### You Will Learn:

- How to assess the insider threat
- How to implement risk-based strategies

Monday, April 4 11:25am-12:25pm

### DSS 2011: Security Program Priorities and Objectives

*Stanley Sims, Director, Defense  
Security Service*

The Defense Security Service is moving ahead on several fronts emphasizing its commitment to enhance and expand the National Industrial Security Program. The recent appointment of Stanley Sims to head the DSS underscores the agency's continued commitment to improving internal operations and external support—both within government and in industry. This timely state of the DSS report will highlight the many changes that have occurred over the past year and provide a window on what to expect in 2011. Topics of discussion will include: deficiency findings from security inspections; FOCI issues and concerns; counterintelligence initiatives; virtual security education and training; cyber security strategy; next generation industrial security automation; information systems security accreditation and anticipated NISPOM changes.

#### You Will Learn:

- Patterns of security deficiencies cited
- Changing security program requirements

*"Every year it just gets better! As a security professional, you just have to attend Impact every year!"*

*Audrey Lavender  
Commonwealth Technology, Inc.*



# AFTERNOON WORKSHOPS

Monday, April 4 2:00pm-3:15pm Track 1

## Track 1 — Security Awareness Training: Critical Success Factors & Techniques

Larry Cunningham, SETA Instructor  
DSS Academy

Employee awareness training is the most cost effective strategy to reduce the overall risk to your organization's classified and sensitive information. It's far more than just annual refresher briefings and a few wall posters — it's about education, culture and structure. The more employees are aware, the greater the chance their behavior will be different, resulting in fewer security incidents. Being able to design, implement and manage an effective security awareness program is a difficult task — even for the best. This “train the trainer” session will walk you through the design of a successful security awareness program. It will address how to overcome various challenges, gain management support, tailor a program to the needs of your workforce, and keep your security message fresh. Learn best practices that have been proven to get results.

### Key Benefits:

- A model for creating a successful awareness program
- How to engage and connect with your audience
- Choosing and using proper awareness techniques

Monday, April 4 3:45pm-5:00pm Track 1

## Track 1 — AIS Security: Compliance Strategies & Best Practices

Paul E. Woodie, Instructor, DSS Academy

Computer technology is rapidly evolving and with every change comes the increased potential for vulnerability. Information security practitioners must stay informed regarding how these changes affect the protection of Automated Information Systems (AIS) and the data stored within them. Identifying and interpreting the myriad NISPOM AIS requirements can be time consuming and overwhelming — never mind determining which plan or procedure best fits your needs. This interactive session will combine extended coverage of changing AIS security requirements and recommended implementation procedures. Whether you're responsible for preparing and implementing information system security plans and policy or providing oversight of your facility's IS used to process classified information, this workshop is for you. Detailed instruction and practical exercises gives you greater understanding of changing security requirements.

### You Will Leave With:

- An in-depth knowledge of current Chapter 8 NISPOM requirements
- Best practices for securing classified information on AIS
- Steps to minimize risk when processing classified data

Monday, April 4 2:00pm-3:15pm Track 2

## Track 2 — OPSEC and Social Media: Lessons from the Trenches

Jeremy H. Duffy, OPSEC Instructor  
Interagency OPSEC Support Staff

The benefits of using social media for business and government are many but there's no getting around the fact that social media also introduces new risks. Significant ones. In an earlier era, “loose lips sink ships” was the military's warning not to let even small details about military movements and operations slip in casual conversation. In contrast, social media Web sites today thrive on loose lips, making it even tougher to maintain operational security. The problem is not so much people twittering away secrets as letting slip many smaller pieces of information that an adversary can piece together. The rapid expansion of social networking sites offer cyber criminals and intelligence collectors a new large target. This session will examine the growing threats posed by social media and how adversaries are exploiting poor operational security practices and what you can do to protect your critical information.

### You Will Learn:

- How to identify and assess critical vulnerabilities
- How to implement an effective protection plan

Monday, April 4 3:45pm-5:00pm Track 2

## Track 2 — Critical Elements of Risk Management and Disaster Planning

Edward Jopeck, VP Government Services  
AcuTech Consulting

The attacks on Sept. 11, 2001 thrust disaster preparedness planning into the spotlight, and subsequent crisis — terrorism bombings in London, the Fort Hood shootings and the recent Tuscon tragedy — are important reminders that all organizations need to have a comprehensive disaster management plan that is ready to roll at a moment's notice. While most organizations will never have an airplane crash into their offices, and most will never be attacked, organizations that are prepared for crisis have an easier time getting back on their feet when disaster does strike. No one can predict when a crisis will hit, but it's security's job to be ready whenever it does. The key is a good plan. Learn how to develop an effective incident response plan before you need it.

### Learn How To:

- Evaluate your organization's risks and vulnerabilities
- Create and implement a successful disaster plan
- Identify resources required for an effective response

**Tuesday  
April 5**

# EDUCATIONAL SESSIONS

Tuesday, April 5 8:10am-8:55am

## National Security in the Age of Wikileaks

Robert "Bear" Bryant, National Counterintelligence Executive

The recent Wikileaks release of thousands of sensitive government documents is raising red flags regarding the risks involved in granting a person access and security clearance to the nation's military secrets. The scale and embarrassment of the leak has caused U.S. officials to redouble efforts to protect against insider threats. In response to breaches in security, the White House is requiring federal agencies to take aggressive new steps to prevent more Wikileaks embarrassments, including instituting "insider threat" programs to ferret out disgruntled employees who might be inclined to leak classified documents. This session will examine the growing threats to national security information posed by unauthorized disclosures of classified information. As the nation's top counterintelligence official, Mr. Bryant will provide an insightful analysis of lessons learned from the Wikileaks scandal and identify key counterintelligence and safeguarding postures needed to protect U.S. secrets.

### You Will Learn:

- Insights from agency vulnerability assessments
- Recommended countermeasures to prevent breaches
- Steps being taken to address the threat

Tuesday, April 5 8:55am-9:40am

## Security Management: Are You Adding or Subtracting Value?

Dee Dee Collins, Executive Director National Security Training Institute

Do you just put out daily fires or are you a full partner in pushing your organization forward and adding to its value? Most security specialists fall somewhere in the middle. No matter what your security job responsibilities may be, the ability to establish rapport quickly, communicate your ideas successfully, and convince others to have confidence in you will decrease your frustration and enable you to achieve your goals. Security professionals have an opportunity and an obligation to add value to their teams and organizations. As with any good sports team, of course, there's no declaring victory until the season is over. And the season is never over for security. Effective leaders know how to get the very best from other people, at every level. This session is designed to help you assess your personal and professional competencies and help you move toward the value side.

### You Will Learn:

- Common traps that cause security pros to fail
- Key attributes of the most successful security managers
- How to measure and demonstrate the value of security

Tuesday, April 5 10:00am-10:45am

## Economic Espionage 2011: Adapting to New Threats

Peter J. Lapp, Chief, Economic Espionage Unit, FBI

As the world's engine room of research and development, the United States is a prime target of foreign spies seeking to steal away critical information — not only military plans and national security secrets but also valuable technological and business trade secrets. At last count, businesses, scientists, students and intelligence agents from nearly 140 countries were trying to get this information. This session will provide a critical overview of the 2011 global economic espionage landscape and the most effective security countermeasures to protect your organization. The FBI's Unit Chief for Economic Espionage will provide an informative briefing on the ever-changing threat vectors used by foreign espionage agents to acquire classified and sensitive national security information.

### You Will Learn:

- Foreign spying capabilities and targets
- Better understanding of your role in counterintelligence
- Heightened awareness of your potential vulnerabilities

Tuesday, April 5 10:45am-11:45am

## Personnel Security Clearances: Issues and Answers

Peregrine D. Russell-Hunter, Dep. Dir., DOHA and Merton Miller, Assoc. Dir., Federal Investigative Services, OPM

The federal government appears to have broken the back of its sluggish security clearance process. Updated statistics show agencies continue to reduce clearance times. While progress has been made to improve timeliness, continued effort is needed to sustain momentum. A new five-tier framework for investigations promises to enable reciprocity of clearances. In this informative Q&A panel session you'll hear from key government players in the security clearance regime about what they're doing to improve the timeliness, reciprocity and quality of security clearances. You'll also hear about the increasing role of technology being deployed to assist in background investigations and the adjudication process. This is your chance to get up to speed on one of the most critical aspects of your security program.

### You Will Learn:

- Automation tools to enhance clearance process
- Adjudication hot button issues
- New developments in security quality metrics

*"Once again the Impact conference proved to be the tour de force venue for security information, education and awareness for government and industry."*

*Paul Schneidmill, U.S. Army RMDA*

# AFTERNOON WORKSHOPS

Tuesday, April 5 1:45-3:00pm Track 1

## Track 1 — Effective Communications: Fine-Tuning Your Briefing Skills

*Martin D. McNair, Corp. Security Specialist, SAIC*

As a security manager, much of your work involves interacting with others and putting your best foot forward. How we communicate and get our security message out to our constituents is vital to the success of our security programs. A poorly designed briefing can ruin your message — and even damage your credibility and reputation. The session will give you practical instruction and guidance on preparing and delivering security presentations. You'll learn how to get your message across, whether you're presenting a security proposal to top management, training your staff or conducting a security briefing for your employees. This power-packed workshop will stimulate your interest and motivate you to seek new paths to improve your communications skills.

### You Will Learn:

- Tips for developing and delivering a speech
- Techniques to motivate your audience
- How to overcome anxiety

Tuesday, April 5 3:20-4:35pm Track 1

## Track 1 — Targeting U.S. Technologies: Trends, Tactics, and Countermeasures

*William D. Stephens, Director, Counterintelligence  
Defense Security Service*

Defense contractors are under constant attack by foreign intelligence services attempting to gather technology secrets. In 2011, foreign spies are expected to step up efforts to obtain classified or restricted U.S. technology. Foreign nations are increasingly exploiting the Internet, including social networking sites, to conduct industrial espionage against DoD contractors. Preventing the unauthorized outward flow of classified technology deployed by the defense industry has become even more difficult in the era of globalization and Wikileaks. Foreign governments and foreign owned commercial entities seek out restricted technologies through a variety of means. This session will examine the findings from the annual DSS report of “suspicious activity” incidents submitted by cleared defense contractors and discuss the current trends, targets and tools of choice being deployed by our adversaries.

### What You'll Learn:

- Foreign intelligence services shopping list
- Current exploitation methods being used
- Countermeasures to protect defense secrets

Tuesday, April 5 1:45-3:00pm Track 2

## Track 2 — Information Systems Certification and Accreditation Clinic

*Randall Riley, Acting Asst. Dep. Dir., ODAA  
Defense Security Service*

Are you experiencing problems getting your information systems approved and accredited for processing classified information? Would you like to complete the process faster and avoid some of the common pitfalls? Then you'll want to make sure you attend this session and learn what you need to know to get your System Security Plan approved and your protection procedures in place. In this interactive workshop, you'll learn about the best practices in preparing your security plan to ensure necessary controls are in place to limit the risk of compromising national security information. You'll find out how to expedite the approval process, ensure that your System Security Plans won't be rejected, and put your cleared personnel to work sooner on these systems.

### You Will Learn:

- Discrepancies found during onsite inspections
- Metrics on common errors found in SSPs
- ODAA initiatives for 2011

Tuesday, April 5 3:20-4:35pm Track 2

## Track 2 — JPAS 2.0: Transitioning for the Future

*Quinton Wilkes, Corp. Security Mgr., L-3 Communications  
Air Force, Navy and Army representatives*

The recent transition of the JPAS system from DSS to the Defense Manpower Data Center (DMDC) has prompted several security enhancements that will be rolled out in early 2011. These enhancements are designed to both improve the security posture of the JPAS system as well as hasten the turnaround time on a number of JPAS functions. As JPAS continues to transition to the future, DMDC will be implementing a “Get Well” plan to address many of the access control, auditing and data quality issues currently plaguing the system. Bring your questions, first-hand experiences and frustrations to this problem-solving workshop where you can get answers from knowledgeable security experts who understand the ins and outs of JPAS and where things are headed. An expert security panel of government and industry JPAS managers will lead you in this highly interactive session.

### Key Benefits:

- New requirements for Common Access Cards
- Planned enhancements to JPAS
- Best practices for using JPAS, JCAVS and e-QIP

**Wednesday  
April 6**

# EDUCATIONAL SESSIONS

Wednesday, April 6 8:10am-8:55am

## **Terrorism 2011: Understanding the New Threat Environment**

*Philip Mudd, Senior Research  
Fellow, New America Foundation*

America faces a dynamic threat that has diversified to a broad array of attacks, from shootings to car bombs to “lone wolf” attacks. There is growing evidence that al-Qaeda is changing its tactics and honing its ability to gather intelligence, employ technology and spot security gaps. Recruitment methods of al-Qaeda have taken full advantage of the Internet in what is referred to as the “cyber jihad.” Homegrown terrorism reflects the changing tactics of al-Qaeda. In this session you will hear first hand about the critical issues facing our country in the fight against terrorism. Philip Mudd, a former senior counterterrorism official with both the CIA and the FBI, will provide an insider’s view of al-Qaeda central and examine the changing nature of the terrorist threat. He will also examine trends now shaping the future of terrorism.

### **You Will Learn:**

- Global terrorism trends and forecast
- Most likely attack scenarios
- Countermeasures to keep pace with evolving threats

Wednesday, April 6 8:55am-9:40am

## **Protecting Classified Networks from Cyber Threats**

*Deborah Plunkett, Dir., Information  
Assurance Directorate, NSA*

The sophistication and volume of attempted security breaches of defense information systems is escalating at a frantic pace. For the Pentagon, which operates 15,000 networks and owns more than a million computers, the risks are huge. Defense systems are attacked constantly — 5,000 times per day by some accounts, and scanned millions of times every day. To date, most cyber attacks have involved espionage. Threats to cyber security show no signs of slowing down in 2011. The vast proliferation of networked devices and computers as well as the increase in the number of mobile workers compounds the government’s cyber security challenges. Managing these increasing risks requires greater collaboration between public and private sectors. This session will explore growing threats on the virtual horizon and how to defend against them.

### **You Will Learn:**

- State of the cyber security threat
- How to defend against computer attacks
- Lessons learned from recent incidents

Wednesday, April 6 10:00am-10:45am

## **State of the National Industrial Security Program**

*William J. “Jay” Bosanko, Director  
Information Security Oversight Office*

As a key player in government security, the Information Security Oversight Office is responsible for oversight of the government-wide security classification system and the National Industrial Security Program. The ISOO director also serves as chair of the National Industrial Security Program Policy Advisory Committee (NISPPAC), which is responsible for recommending changes in industrial security policy and the National Industrial Security Program Operating Manual. Staying up to date with critical policy issues should be a key part of your security strategy this year. This timely session will bring you up to speed on the latest and most important issues affecting government security and the National Industrial Security Program. Find out what hot button issues will drive the NISP in 2011.

### **Key Issues:**

- NISPPAC working groups’ agenda for 2011
- Recent and upcoming policy changes
- Update on controlled unclassified info rules

Wednesday, April 6 10:45am-11:45am

## **Defending Against China’s Economic Espionage Prowess**

*Peter Mitchener, Sr. China Analyst  
Federal Bureau of Investigation*

U.S. counterintelligence officials identify China as one of the most aggressive collectors of sensitive technology and secrets. Last year alone, 11 Chinese espionage cases were prosecuted in the United States, the highest number yet, and they featured a wide range of espionage targets including dual civilian-military technology, proprietary corporate data and military technology. China recently unveiled a new, high-tech stealth fighter and some of its technology, it turns out, may have well come from the U.S. itself. One thing is certain: Chinese espionage activities will continue apace in 2011. Recent incidents and case studies offer insights into clandestine operational methods employed by the Chinese Intelligence Services and demonstrate China’s patient and purposeful approach to espionage. This session will examine the changing threat of Chinese spying and how China’s spies operate against the U.S.

### **You Will Learn:**

- Key trends from recent case studies
- Scope of Chinese spying in U.S.
- Top targets, tactics and methods used



*“Thoroughly enjoyed the event. I learned a lot and received many tools to carry out my plan for security.”*

*Stephanie Isom  
General Dynamics – AIS*

# AT-A-GLANCE

## THREE DAYS OF

# CAREER-CRITICAL INFORMATION



### Monday, April 4

7:00 — 7:50 am.	Registration. Coffee and pastry will be served during registration
7:50 — 8:00 am.	Welcome and Opening Remarks
8:00 — 8:45 am.	<b>Defending Against Cyber Threats in Dangerous Times</b> Gen. Michael V. Hayden, Principal, Chertoff Group, Former Director CIA, NSA
8:45 — 9:40 am.	<b>Russian Espionage: The Bear Is Back</b> Oleg Kalugin, Former KGB Major General, CI Centre Professor
9:40 — 10:40 am.	Refreshment Break, Security Awareness Fair and Expo
10:40 — 11:25 am.	<b>The Insider Threat: Confronting A New World of Risk</b> Ira Winkler, President, Internet Security Advisors Group
11:25 — 12:25 pm.	<b>DSS 2011: Security Program Priorities and Objectives</b> Stanley Sims, Director, Defense Security Service
12:30 — 2:00 pm.	Host Networking Luncheon, Security Awareness Fair and Expo
2:00 — 3:15 pm.	<b>Track 1: Security Awareness Training: Critical Success Factors &amp; Techniques</b> Larry Cunningham, SETA Instructor, DSS Academy <b>Track 2: OPSEC and Social Media: Lessons from the Trenches</b> Jeremy H. Duffy, OPSEC Instructor, Interagency OPSEC Support Staff
3:15 — 3:45 pm.	Refreshment Break, Security Awareness Fair and Expo
3:45 — 5:00 pm.	<b>Track 1: AIS Security: Compliance Strategies &amp; Best Practices</b> Paul E. Woodie, Instructor, DSS Academy <b>Track 2: Critical Elements of Risk Management and Disaster Planning</b> Edward Jopeck, VP Government Services, AcuTech Consulting

### Tuesday, April 5

7:00 — 8:00 am.	Coffee and Pastry
8:00 — 8:10 am.	Opening Remarks
8:10 — 8:55 am.	<b>National Security in the Age of Wikileaks</b> Robert "Bear" Bryant, National Counterintelligence Executive
8:55 — 9:40 am.	<b>Security Management: Are You Adding or Subtracting Value?</b> Dee Dee Collins, Executive Director, National Security Training Institute
9:40 — 10:00 am.	Refreshment/Networking Break
10:00 — 10:45 am.	<b>Economic Espionage 2011: Adapting to New Threats</b> Peter J. Lapp, Chief, Economic Espionage Unit, FBI
10:45 — 11:45 pm.	<b>Personnel Security Clearances: Issues and Answers</b> Peregrine D. Russell-Hunter, Dep. Dir., DOHA Merton Miller, Assoc. Dir., Federal Investigative Services, OPM
12:15 — 1:45 pm.	Host Networking Luncheon
1:45 — 3:00 pm.	<b>Track 1: Effective Communications: Fine-Tuning Your Briefing Skills</b> Martin D. McNair, Corp. Security Specialist, SAIC <b>Track 2: Information Systems Certification and Accreditation Clinic</b> Randall Riley, Acting Asst. Dep. Dir., ODAA, Defense Security Service
3:00 — 3:20 pm.	Refreshment/Networking Break
3:20 — 4:35 pm.	<b>Track 1: Targeting U.S. Technologies: Trends, Tactics &amp; Countermeasures</b> William D. Stephens, Director, Counterintelligence, Defense Security Service <b>Track 2: JPAS 2.0: Transitioning for the Future</b> Quinton L. Wilkes, Corp. Security Mgr., L-3 Communications Representatives from Army, Navy and Air Force

*"This was an excellent conference. Good topics, presenters and an excellent opportunity to network and develop contacts."*  
Stephen Miller  
New Mexico University



### Wednesday, April 6

7:00 — 8:00 am.	Coffee and Pastry
8:00 — 8:10 am.	Opening Remarks
8:10 — 8:55 am.	<b>Terrorism 2011: Understanding the New Threat Environment</b> Philip Mudd, Senior Research Fellow, New America Foundation
8:55 — 9:40 am.	<b>Protecting Classified Networks from Cyber Threats</b> Deborah Plunkett, Dir., Information Assurance Directorate, National Security Agency
9:40 — 10:00 am.	Refreshment/Networking Break
10:00 — 10:45 am.	<b>State of the National Industrial Security Program</b> William J. "Jay" Bosanko, Director, Information Security Oversight Office
10:45 — 11:45 am.	<b>Defending Against China's Economic Espionage Prowess</b> Peter Mitchener, Sr. China Analyst, FBI
11:45 — 11:50 am.	Closing Remarks

# REGISTER EARLY & SAVE

## FOUR EASY WAYS TO REGISTER

# 4

1. Register online at: <http://nsi.org/Impact-2011.html>
2. Fax the registration form with payment information to: (508) 507-3631
3. Mail the registration form and payment to:  
National Security Institute  
165 Main St., Ste 215  
Medway, MA 02053
4. Call (508) 533-9099

## REGISTER EARLY AND SAVE \$50

### Earlybird Discount

A special rate of \$845 is being offered to all attendees whose payment is received by February 28, 2011. The registration fee covers all program materials, admission to pre- and post-conference workshops, host reception, luncheons and refreshment breaks.

### Regular Rate

The fee for registrations received after February 28, 2011 is \$895. All registrations must be accompanied by a check made payable to the National Security Institute, a Purchase Order or Government Training Form. You may also charge your MasterCard, Visa or American Express.

### Cancellation Policy

Cancellations must be made in writing to the National Security Institute. Refunds for cancellations received on or before March 15th will be subject to a \$50 administrative fee. Cancellations received after March 15, 2011 will forfeit 100 percent of the total conference fee. Substitutions may be made at any time by calling NSI.

### Conference Hours

#### Monday, April 4

Registration 7:00 am. – 7:50 am.

Conference 7:50 am. – 5:00 pm.

Networking Reception 5:00 pm. – 6:00 pm.

#### Tuesday, April 5

Conference 8:00 am. – 4:35 pm.

#### Wednesday, April 6

Conference 7:50 am. – 11:55 am.

### Pre-Conference Workshop

Sunday, April 3, 2:00 pm. – 5:00 pm.

### Security Awareness Fair and Expo

Monday, April 4, 9:40 am. – 3:45 pm.

### Meeting Attire

Attire for the National Security Institute Conference and Exhibition is business casual.



### Hotel Reservations

To reserve your room call Marriott reservations at 1-800-228-9290 or reserve your room online at [https://resweb.passkey.com/Resweb.do?mode=welcome\\_gi\\_new&groupID=2618524](https://resweb.passkey.com/Resweb.do?mode=welcome_gi_new&groupID=2618524). When calling,

please ask for the NSI IMPACT 2011 rate at the Westfields Marriott in order to receive the discounted group rate of \$209. The group rate will be available until March 11th or until the group block is sold-out, whichever comes first. Please be aware the room block fills quickly, so we suggest you make your hotel and travel plans early.

The Westfields Marriott is located at 14750 Conference Center Drive, Chantilly, Virginia, 20151. The Westfields Marriott hotel combines sophisticated meeting facilities with elegant hotel accommodations and also features access to the Westfields Signature Fred Couples Golf Club.

## About NSI

Founded in 1985, the National Security Institute (NSI) is a publisher and educator serving the needs of security professionals in government, the corporate sector, and defense contracting. We publish newsletters and special reports, we sponsor seminars and conferences, and we offer government and industry security professionals a FREE e-newsletter, delivering national and international news pertinent to the security profession. We produce the industry's most respected and cost-effective security awareness services. Visit us at <http://nsi.org>.

# REGISTRATION FORM

**REGISTER BY  
FEB 28  
AND  
SAVE  
\$50!**

## Who Should Attend IMPACT 2011...

- ◆ Facility Security Officers
- ◆ Government Personnel Security Managers
- ◆ Corporate Security Directors
- ◆ Information Security Managers
- ◆ Classification Management Specialists
- ◆ AIS Security Managers
- ◆ Security Education and Training Specialists
- ◆ Government Agency Security Specialists
- ◆ Classified Material Control Specialists
- ◆ Information System Security Managers
- ◆ OPSEC Managers
- ◆ Security Policy Adjudicators
- ◆ JPAS Account Managers

### Platinum Sponsor



### Gold Sponsors



## Priority Registration Form

## IMPACT 2011

**PROTECTING SECRETS: Confronting A New World of Risk**  
Chantilly, Virginia, April 4 - 6, 2011

Please print, type or attach your business card and forward to: National Security Institute, 165 Main Street, Suite 215, Medway, MA 02053. Tel: 508-533-9099  
Fax: 508-507-3631. Photocopy for additional registrations.

Name: \_\_\_\_\_ Title: \_\_\_\_\_

Company/Agency: \_\_\_\_\_

Address: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_

Phone: \_\_\_\_\_ E-mail: \_\_\_\_\_

Enroll me in the JPAS User Training Workshop on Sunday, April 3, 2:00 - 5:00 pm

**Note:** This workshop is available to all three-day conference registrants.

### Method of Payment

Check Enclosed  Purchase Order/1556 Form Enclosed  
Charge to Credit Card:  VISA  Mastercard  AMEX

Card No. \_\_\_\_\_ Exp. Date \_\_\_\_\_

Name on Card \_\_\_\_\_

Authorized Signature \_\_\_\_\_

### Registration Fees

	Rcvd. by 2/28/11	After 2/28/11
3-day Registration	<input type="checkbox"/> \$845	<input type="checkbox"/> \$895
2-day Registration	<input type="checkbox"/> \$795	<input type="checkbox"/> \$795
1-day Registration	<input type="checkbox"/> \$545	<input type="checkbox"/> \$545

*"This is my fifth NSI Impact conference and the conference has never failed in meeting my expectations. Always informative, always relevant, and always enjoyable!"*

*Karen V. Gunter, U.S. Army,  
Radford Army Ammunition Plant*



165 Main Street, Suite 215  
Medway, MA 02053

First Class  
Presort  
US Postage  
PAID  
N. Reading, MA  
Permit No. 140

## Why IMPACT 2011 Will be Your Most Critical Professional Experience of the Year

- You'll get up to date on the hottest security issues: security clearances, JPAS, NISP, AIS security, economic espionage, cyber security threats, security awareness, terrorism, OPSEC.
- You'll return to your office with an entire reference library that will put the information you need at your fingertips: binder, DVD, follow-up e-mails!
- You'll gain networking contacts you can call on all through the year: make friends; get to know the major figures in your profession.
- You'll learn about key developments of the past year — and what to expect in the year ahead — in a relaxed atmosphere conducive to education!
- You'll be prepared to handle all aspects of JPAS, with more than 4 hours of in-depth training offered.
- You'll learn security's latest best practices... and return to your office prepared to implement solutions before they are needed and eliminate security vulnerabilities before they happen!
- You'll spend 3 days with people who understand and care about what you do every day because they do it, too!

### 12 Special Features of IMPACT 2011

- ◆ In-depth, practical workshops, not PowerPoint snooze-a-thons!
- ◆ Briefings with important heads of government agencies
- ◆ 2011 Edition of NSI's Reference Data Library on DVD
- ◆ Sessions targeted to personal and professional development, will help you become better at your job
- ◆ Comprehensive pre-conference JPAS workshop
- ◆ NSI's 2011 Security Awareness Fair and Expo
- ◆ Reception, luncheons, and refreshment breaks with your colleagues
- ◆ Outstanding speakers and session presenters
- ◆ Post-conference session updates via e-mail
- ◆ Sessions new for 2011 to address the hottest security topics
- ◆ Excellent, business-class hotel, minutes from major airports
- ◆ Take-away binder of conference program materials