Safeguarding U.S. Secrets in the Cyber World
Prepare for Changes Ahead at Impact ‘19

Join the best minds in government and industry security for three innovative days at NSI’s 34th Annual IMPACT ’19 Seminar and Expo on April 15 - 17 at the Westfields Marriott in Chantilly, Virginia.

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 the skills and resources needed to make you indispensable at your job.

At IMPACT ’19, you’ll gain a comprehensive, 360-degree view of changing security threats, new compliance strategies and best-in-class solutions. Led by a top-flight faculty of speakers and trainers, IMPACT ’19 features an impressive line-up of security threat briefings, training workshops, case studies and practical take-home tools to improve your security program.

Informative Sessions, Practical Workshops and Networking


Learn everything you need-to-know from over 21 leading government and industry security experts at IMPACT ’19 — the one seminar you and your security team can’t afford to miss this year.

FREE BONUS WORKSHOP:

Pre-Seminar DISS Training
Sunday, April 14, 2:00 pm – 5:00 pm
Open to seminar attendees only,
this three-hour bonus workshop will help you to successfully navigate the transition to the new Defense Information System for Security (DISS). This practical training session provides a hands-on demonstration of the new clearance data system that replaces JPAS. This complimentary workshop is available to three-day registrants only.

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 2019 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 2019 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 2019 offers small, more intimate sessions that bring you closer to the action and the speakers as well as your peers.

“I have been attending this seminar since 2000. I’ve met many new people who I can network with in the future. The speakers are excellent and provide pertinent information.”

Mary Albrecht
Oshkosh Defense, LLC
Reasons to Attend

1. Top Speakers, Targeted Topics
All speakers are 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 security requirements.

2. It’s What You Asked for
We extensively surveyed hundreds of top security professionals to deliver the tailored solutions to the most important challenges you face now… and throughout 2019.

3. 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, and sessions for beginners through veteran security practitioners.

4. Practical, In-Depth Workshops
Interactive workshops provide extended training in critical security areas like NISP compliance; clearance processing; counterintelligence; cyber security; insider threat programs; security awareness; security case studies, and real-world lessons learned.

5. 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 2019 Security Awareness Fair and Expo. The major government security agencies will be there offering a broad array of complimentary materials and media through their security outreach programs. These complimentary resources are ready to take home to implement in your organization.

A Sampling of the 2019 Exhibitors

Valuable Take-Home Resources
Every IMPACT 2019 registrant goes home with a comprehensive binder of seminar materials and handouts and a DVD containing the 2019 Edition of NSI’s Reference Library.

This remarkable DVD is packed with articles, white papers, checklists, glossaries, reports, surveys, and primary sources.

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.

Champagne Reception
MONDAY, APRIL 15, 5:00 - 6:30PM
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.
I look forward to the Impact security forum every year! I walk away with a better understanding and clarification on topics that effect my job directly.

LaChaka Treakle
ICF
Track 1 — Security Awareness: Keeping Your Program Relevant and Engaging

Tom Brown, Director, Govt. Security
AECOM

Awareness is a powerful tool in creating a strong security culture and influencing organizational behavior. But few awareness programs are delivering on their intended impact as employee missteps and insider threats continue to dominate the headlines. So how do you change employee behavior and empower your workforce with the security know-how to help protect government and company secrets? This workshop will offer insights on how to create relevant awareness content that keeps your employees engaged.

You Will Learn:
- How to create awareness programs that people won’t hate
- Critical factors that lead to high-impact awareness
- Marketing techniques that get employee buy-in

Track 2 — Navigating the NBIS and the NISS

Dr. Chuck Barber, Dir., Enterprise Bus. Support Office, Defense Vetting Directorate
Heather Green, Dir., Vetting Risk Operations, Defense Vetting Directorate
Ryan Deloney, Asst. Deputy Director, Industrial Security Field Ops., DSS

There are many changes on the horizon in the Personnel Security Vetting mission space. The National Background Investigation Services (NBIS) is the enterprise infrastructure that encompasses all of the Personnel Security Vetting systems. Initiatives are underway to transform how personnel security clearance and suitability data are collected, processed, reviewed, and shared. The Defense Vetting Directorate of the Defense Security Service is leading this change with the establishment of their Enterprise Business Support Office and the Vetting Risk Operations Center. This comprehensive workshop will address the issues associated with successfully navigating these new security systems, organizations and processes.

You Will Learn:
- Rules of the road to navigate the NBIS and the NISS
- How centralized vetting operations will achieve efficiencies

Track 1 — Creating an Effective Travel Security Program

Mathew Bradley, Reg. Security Dir., Americas
International SOS

In a world where international travel is growing faster than ever before and the risk landscape for travelers continues to change, having a robust travel risk management program in place is key in order to fulfill your duty of care to employees, and to maintain organizational resilience. Without a clearly defined and communicated travel risk management program in place, you’re potentially putting traveling employees in harm’s way, which can have serious operational, reputational, financial and legal repercussions for your organization. The threats today can affect anyone, anywhere.

You Will Learn:
- Global emerging travel threats
- Risk analysis and sources of information
- Practical risk mitigation strategies

Track 2 — How to Comply with the DSS Risk Management Framework


The Risk Management Framework is a significant undertaking for most organizations and all defense contractors with classified information systems must comply with the six-step RMF process in order to receive or maintain their system authorization. This new accreditation process provides a complex challenge to industry through new approaches to system categorization, assessment and continuous monitoring. Understanding these requirements along with the RMF process is key to getting your information systems approved. Navigating the complex Risk Management Framework requirements can be daunting. Learn best practices and gain a better understanding of RMF.

You Will Learn:
- How to obtain timely authorizations
- Key missteps to avoid
- Steps and tools in the RMF process
Tuesday, April 16

**U.S. Secrets Under Siege from Nation-State Hackers, Spies**
William Evanina, National CI Executive Director, NCSC

It’s alarming, but no exaggeration, to say the nation is facing the most challenging and significant foreign intelligence entity threat in its history. The foreign spying threat is increasing in both scale and sophistication. Today’s spy threat includes both cyber operations and influence activities, in addition to traditional spying by nations such as China and Russia. Every day U.S. government and defense contractors are targeted by nation-state actors for espionage and theft, resulting in huge losses of national security information and technology secrets. Staying ahead of the threat requires constant vigilance.

**You Will Learn:**
- How to defend against growing threats
- Countermeasures to protect secrets
- Current exploitation methods being used

**DoD Security Program Policy Update**
Garry P. Reid, Director for Defense Intelligence, DoD Intelligence and Security, OUSD

The rapid and substantive changes in the nation’s security program have major impacts on the way security professionals implement and plan for these requirements. Within the Department of Defense the schedules for implementation of various elements of these requirements as well as new policies and procedures are included in the mission of the Director of Defense Intelligence (DoD Intelligence and Security). The mission includes collaboratively developing innovative methods for assessing risk in the workforce and crafting mitigation strategies to protect people, information and programs from insider and outsider threats.

**You Will Learn:**
- New DoD security initiatives
- Policy plans and phased implementation
- Key challenges ahead

---

**Security Clearance Program Transition: What to Expect**
Charles Phalen, Director, NBIB
Perry Russell-Hunter, Director, DOHA
Tricia Stokes, Dir., Defense Vetting Directorate, DSS

The National Background Investigations Bureau (NBIB) is in the midst of planning to transition their facilities, workloads and 2,000 employees to the Defense Security Service by Oct. 1, 2019, pending a presidential executive order. The consolidation will help ensure the continuing progress being made to reduce the security clearance backlog. Several transformation initiatives are in the works including new initiatives to implement continuous evaluation, reducing the need for periodic reinvestigations.

**You Will Learn:**
- Current reforms underway and what they mean to you
- Processes to improve the security clearance system
- Plans and timelines to resolve clearance backlog

---

**Insider Threat Prevention, Detection, Mitigation and Deterrence**
Dr. Michael Gelles, Managing Director, Deloitte Consulting

Organizations continue to face a variety of insider threats, as demonstrated by a string of high profile cases where employees have used their knowledge and access to physical and/or information systems to cause significant damage. These cases highlight vulnerabilities and underscore a historical perception that insider threat mitigation is predominately a cyber-security challenge, and categorized as a strictly information technology responsibility. This approach unfortunately can leave your organization vulnerable to existing and emerging insider threats. Effective risk mitigation requires a different approach where insider threats are addressed as part of a holistic and risk-based program.

**You Will Learn:**
- Analysis of behavioral indicators
- Elements of effective insider threat program

---

“The speakers were excellent and really conveyed their knowledge effectively. Great topics with just the right amount of time for each.”

Kelly Batchelder-Long
DOJ/FBI
Track 1 — CUI Compliance: How to Get It Right
Mark Riddle, Senior Program Analyst
Information Security Oversight Office

Classified information usually gets all the attention, but “Controlled, Unclassified Information” or CUI addresses the way controlled information is marked and disseminated in non-classified documents. The CUI Program addresses the current inefficient and confusing patchwork of over 100 agency-specific policies throughout the executive branch that lead to inconsistent marking and safeguarding as well as restrictive dissemination policies. This workshop will help you get out in front of this compliance issue and develop a baseline of knowledge to create a plan to properly protect controlled, unclassified information.

You Will Learn:
- Develop a CUI compliance plan
- Special marking and handling requirements
- CUI milestones and timeline

Track 2 — Assessing Your Insider Threat Program
Daniel McGarvey, Sr. Principal Bus. Process Analyst
Alion Science & Technology

The Director of National Intelligence’s (DNI) “National Insider Threat Task Force” (NITTF) has issued their maturity framework to help NISP program managers ensure their insider threat programs meet certain baseline criteria. Six areas of focus within the maturity framework include: Senior Official/Insider Threat Program Leadership; Program Personnel; Employee Training and Awareness; Access to Information; Monitoring User Activity; and Information Integration, Analysis, & Response. This workshop provides a benchmark against which your organization can evaluate the capability of its insider threat program and set goals and priorities for improvement.

You Will Learn:
- Steps to building an insider threat program
- How to gain buy-in from key stakeholders
- Lessons learned from the experts

Track 1 — DSS Industrial Security Program Issues and Answers
Gus E. Greene, Director, Industrial Security, Defense Security Service

Ongoing changes in the National Industrial Security Program mean that FSOs will have more compliance issues to contend with in 2019. DSS vulnerability assessments have broadened their scope to include insider threat programs and new information system security mandates. Keeping up with changing requirements and knowing where potential problems lie is critical to avoid security compliance issues and safeguard classified information. This interactive Q&A session will guide you through the compliance issues you face in meeting NISPOM requirements. You’ll also find out what red flags IS reps are encountering during their contractor assessment visits.

You Will Learn:
- Hands-on advice for keeping your program in compliance
- Industrial security program initiatives for 2019
- How to achieve a superior security rating

Track 2 — Preparing for an Active Shooter Emergency in the Workplace
Capt. Douglas Watson, Winchester Police Dept.
SWAT Team Coordinator

According to a recent FBI study, nearly half of all active shooter situations happen in the workplace. While it’s never pleasant to think about these things, it is imperative that all businesses and organizations have an emergency action plan (EAP) in place. An EAP not only outlines the responsibilities and what to do in a high-stress situation, but also results in faster response times and gives employees a level of security because they know what to do and how to respond. This workshop will help you prepare for a worst-case scenario at your facility or organization.

You Will Learn:
- Ways to prevent and survive an attack
- Key elements of an action plan
- Best practices for success
Chinese Espionage: Growing Risks to U.S. Defense Companies
FBI Counterintelligence Division

Chinese economic espionage as well as efforts to steal U.S. research and technology amount to the most severe counterintelligence threat facing the United States today, according to the FBI. In fact, China was involved in 90% of all economic espionage cases handled by the Department of Justice over the last seven years. Counterintelligence officials believe China’s espionage activity has been increasing over the past few years and see no decline in the foreseeable future.

You Will Learn:
- Latest trends in China’s spying activities
- What (and who) is being targeted
- Effective and practical countermeasures

Low-Tech Threats: Protecting the People Side of Security
Ryan Kalember, Sr. VP of Cybersecurity Strategy Proofpoint, Inc.

Low-tech threats often lead to high-profile breaches. Many of the most recent, notable cyber attacks were not caused by high-tech espionage. Rather, they were the product of low-tech social engineering targeting the most vulnerable aspect of security — people. For the foreseeable future, low-tech social engineering hacking will continue to be a dominant cyber risk. If anything, it is likely to proliferate across growing and emerging technology platforms – mobile and other Internet-enabled devices (Internet of Things) and social media. This session focuses on everyday hacks and insider threats that, while simple in nature, actually add up to the most significant losses.

You Will Learn:
- Common techniques and how to prevent an attack
- How to defend against common low-tech attacks

Annual State of the National Industrial Security Program
Mark A. Bradley, Director, Information Security Oversight Office

The National Industrial Security Program (NISP) is undergoing significant changes in several key areas that will dictate future requirements for the protection of classified and sensitive unclassified information. The Information Security Oversight Office (ISOO), which oversees the government-wide security classification system and the National Industrial Security Program, is at the forefront of these efforts. As changes to industrial security policy advance, security practitioners can take a number of steps now to address changing requirements and stay ahead of coming reforms. This timely presentation will bring you up to speed on key areas of government security that will affect the way you do your job.

You Will Learn:
- Understand changing security requirements
- NISPOM revision and update
- What’s on the NISPPAC agenda for 2019

Showing How Security Is a Value-Add to Your Organization
Mitchell Lawrence, National Security Training Institute; CEO, Lawrence Solutions

The role of security professionals has become increasingly complex—and is likely to become even more complicated in the foreseeable future. The biggest challenge security teams face in their organization is one of perception and how to communicate value. Effectively communicating value to your stakeholders is critical for your organization to achieve its objectives, whether it’s to convince management to increase security funding or change corporate culture to minimize costly, security-robbing behaviors. This session will show you how to create, communicate and achieve value in your role and at your organization.

You Will Learn:
- Understand the business case for security
- How to create and communicate value
- Showcase security’s positive impact

“Very professional! One of the better seminars I have attended. Presenters, materials, facilities all excellent.”

Michael Alvarez
Naval Special Warfare Command
**Monday, April 15**

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. **Countering Evolving Threats to National Security**
                Charles (Chuck) Durant, Deputy Director for Counterintelligence, DOE
8:45 — 9:30 am. **Terrorism and Security: Mapping The Risks in 2019**
                Peter Bergen, VP, Global Studies & Fellows, New America
9:30 — 10:30 am. Opening of Awareness Fair, Expo and Refreshment Break
10:30 — 11:30 am. **Changing Nature of Cyber Threats: What FSOs Need to Know**
                   Christopher Krebs, Director, DHS Cybersecurity and Infrastructure
11:30 — 12:30 pm. **DSS: Developing a Risk-Based Approach To Industrial Security**
                    Daniel E. Payne, Director, Defense Security Service
12:40 — 2:00 pm. Host Networking Luncheon, Security Awareness Fair and Expo
2:00 — 3:15 pm. **Track 1 – Security Awareness: Keeping Your Program Relevant and Engaging**
                 Tom Brown, Director, Govt. Security, AECOM
                 **Track 2 – Successfully Navigating the Changing DISS and NISS**
                 Dr. Chuck Barber, Dir., Enterprise Bus. Support Office, Defense Vetting Directorate;
                 Heather Green, Dir., Vetting Risk Operations, Defense Vetting Directorate
                 Ryan Deloney, Asst. Deputy Director, Industrial Security Field Ops., DSS
3:15 — 3:35 pm. Refreshment Break, Security Awareness Fair and Expo
3:35 — 4:50 pm. **Track 1 – Creating an Effective Travel Security Program**
                 Mathew Bradley, Reg. Security Dir., Americas International SOS
                 **Track 2 – How to Comply With the DSS Risk Management Framework**

---

**Tuesday, April 16**

7:00 — 7:50 am. Coffee and Pastry
7:50 — 8:00 am. Opening Remarks
8:00 — 8:45 am. **U.S. Secrets Under Siege from Nation-State Hackers, Spies**
                 William Evanina, National CI Executive Director, NCSC
8:45 — 9:30 am. **DoD Security Program Policy Update**
                 Garry P. Reid, Dir. Defense Intelligence, DoD Intel and Security, OUSD
9:30 — 9:50 am. Refreshment/Networking Break
9:50 — 10:50 am. **Security Clearance Program Transition: What to Expect**
                   Charles Phalen, Director, NBIB; Perry Russell-Hunter, Director,
                   DOHA & Tricia Stokes, Dir., Defense Vetting Directorate, DSS
10:50 — 11:50 am. **Insider Threat Prevention, Detection, Mitigation and Deterrence**
                    Dr. Michael Gelles, Managing Director, Deloitte Consulting
12:00 — 1:30 pm. Host Networking Luncheon
1:30 — 2:45 pm. **Track 1 – CUI Compliance: How to Get It Right**
                 Mark Riddle, Senior Program Analyst, Information Security Oversight Office
                 **Track 2 – Assessing Your Insider Threat Program**
                 Daniel McGarvey, Sr. Principal B us. Process Analyst, Alion Science & Technology
2:45 — 3:05 pm. Refreshment/Networking Break
3:05 — 4:20 pm. **Track 1 – DSS Industrial Security Program Issues and Answers**
                 Gus E. Greene, Director, Industrial Security, Defense Security Service
                 **Track 2 – Preparing for an Active Shooter Emergency in the Workplace**
                 Capt. Douglas Watson, Winchester Police Dept., SWAT Team Coordinator

---

**Wednesday, April 17**

7:00 — 7:50 am. Coffee and Pastry
7:50 — 8:00 am. Opening Remarks
8:00 — 8:45 am. **Chinese Espionage: Growing Risks to U.S. Defense Companies**
                 FBI Counterintelligence Division
8:45 — 9:30 am. **Low-Tech Threats: Protecting the People Side of Security**
                 Ryan Kalember, Sr. VP of Cybersecurity Strategy, Proofpoint, Inc.
9:30 — 9:50 am. Refreshment/Networking Break
9:50 — 10:35 am. **Annual State of the National Industrial Security Program**
                   Mark Bradley, Director, Information Security Oversight Office
10:35 — 11:35 am. **Showing How Security Is a Value-Add to Your Organization**
                   Mitchell Lawrence, National Security Training Institute; CEO, Lawrence Solutions
11:35 — 11:45 am. Closing Remarks
Seminar Hours
Monday, April 15
Registration 7:00 am.–7:50 am.
Conference 7:50 am.–4:50 pm.
Networking Reception 5:00 pm.–6:30 pm.
Tuesday, April 16
Conference 7:50 am.–4:20 pm.
Wednesday, April 17
Conference 7:50 am.–11:45 am.

Pre-Conference Workshop
Sunday, April 14, 2:00 pm.–5:00 pm.

Security Awareness Fair and Expo
Monday, April 15, 9:30 am.–3:35 pm.

Meeting Attire
Attire for the National Security Institute’s Impact Forum and Exhibition is business casual.

Hotel Reservations
To reserve your room call Marriott reservations at 1-877-212-5752 or reserve your room online at https://book.passkey.com/event/49745439/owner/13564/home. When calling, please ask for the NSI IMPACT 2019 rate at the Westfields Marriott in order to receive the discounted group rate of $239. The group rate will be available until March 23rd 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 veteran-owned 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.
Who Should Attend IMPACT 2019…

- Facility Security Officers
- Information System Security Professionals
- Government Personnel Security Managers
- Corporate Security Directors
- Information Security Managers
- Classification Management Specialists
- Counterintelligence Professionals
- Security Education and Training Specialists
- Government Agency Security Specialists
- Classified Material Control Specialists
- OPSEC Managers
- Security Adjudicators
- DISS Account Managers

Priority Registration Form

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: ______________________________________

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

<table>
<thead>
<tr>
<th></th>
<th>Rcvd by 3/1/19</th>
<th>After 3/1/19</th>
</tr>
</thead>
<tbody>
<tr>
<td>3-day Registration</td>
<td>$945</td>
<td>$995</td>
</tr>
<tr>
<td>2-day Registration</td>
<td>$845</td>
<td>$845</td>
</tr>
<tr>
<td>1-day Registration</td>
<td>$595</td>
<td>$595</td>
</tr>
</tbody>
</table>

Gold Sponsors

- MATHCRAFT
- SECUrites
- ThreatSwitch
- NSTI

IMPACT 2019

Safeguarding U.S. Secrets in the Cyber World

Chantilly, Virginia, April 15 - 17, 2019

Enroll me in the Defense Information System for Security (DISS) Workshop

Sunday, April 14, 2:00 - 5:00 pm

Note: This complimentary workshop is available to all three-day Impact registrants.
You’ll get up to date on the hottest security issues: security clearances, DISS, NISP, classified systems security, economic espionage, cyber security threats, security awareness, terrorism, insider threats.

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 the transition to DISS, with four 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!

Why IMPACT 2019 Will be Your Most Critical Professional Experience of the Year

- In-depth, practical workshops, not PowerPoint snooze-a-thons!
- Briefings with important heads of government agencies
- 2019 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 Defense Information System for Security (DISS) workshop
- NSI’s 2019 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 2019 to address the hottest security topics
- Excellent, business-class hotel, minutes from major airports
- Take-away binder of conference program materials