Reshaping Government Security For a New Decade

New for 2020...

★ Threat Forecast and Top Security Challenges
★ NISP Compliance Mandates and Best Practices
★ DCSA’s Expanded Mission and How It Affects You
★ Emerging Cyber Risks to Classified Information
★ Security Program Roadmap for the Future

Plus: Pre-Conference DISS Workshop
Reshaping Government Security For a New Decade

There are big changes taking place in the National Industrial Security Program and NOW is the time to prepare for what lies ahead.

From the transition to a risk-based model of security to the transformation of the security clearance process, there are a host of new challenges and compliance issues you’ll have to contend with.

To keep pace, your security program must evolve while at the same time counter a growing array of threats — both inside and outside — as corporate and government secrets become more vulnerable than ever.

Get the training you need to prepare yourself and your security team for the challenges you’ll face in 2020.

Join the best minds in government and industry security for three innovative days at NSI’s 35th Annual IMPACT ’20 Seminar and Expo on April 20-22 at the Westfields Marriott in Chantilly, VA.

Learn the “How-to” at IMPACT ’20

Learn everything you need-to-know from over 21 leading government and industry security experts at IMPACT ’20 — the one forum you and your security team can’t afford to miss this year.

Led by a top-flight faculty of speakers and trainers, IMPACT ’20 features an impressive line-up of security threat briefings, training workshops, case studies and practical take-home tools to improve your program and prepare you for the security road 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.

FREE BONUS WORKSHOP:

Pre-Seminar DISS Training
Sunday, April 19, 2:00pm–5:00pm
This three-hour complimentary workshop will help you successfully navigate the transition to the new Defense Information System for Security. This bonus workshop is available to three-day registrants only.

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

“I enjoy attending the Impact seminar each year. Presenters, material and venue is excellent! I always take back good information to my organization each year.”

Pam Spilman
SAIC
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 2020.

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 2020 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 2020 Exhibitors**

**Valuable Take-Home Resources**

Every IMPACT ’20 registrant goes home with a comprehensive binder of seminar materials and handouts and a DVD containing the 2020 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 20, 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.
Assessing the National Security Threat Landscape for 2020
William Evanina, Director, National Counterintelligence & Security Center

The rapidly evolving national security landscape proves that threat actors remain undeterred from seeking classified information and technology. From nation-state espionage to cyberattacks and insider threats, the security risks we face as a nation have never been greater or more diverse.

As today’s threat-intensive environment becomes more hostile with each passing day, it is vital for you to be equipped with the tools, techniques and knowledge needed to safeguard national security information from damaging breaches. In this scene-setting keynote address, find out what threats are on the horizon for 2020 and how to safeguard your organization’s critical information.

Confronting the Cyber Security Challenge: What More Can You Do?
Bryan S. Ware, Asst. Director
Cybersecurity & Infrastructure Security Agency, DHS

Cyber-attacks against government networks are growing more sophisticated, frequent and dynamic. The cyber espionage threat from nation-states—including China and Russia—calls for a new mode of collaboration with the private companies that are now on the front lines. To tackle the constantly evolving challenge of protecting the United States from these attacks, DHS established the Cybersecurity & Infrastructure Security Agency to protect the nation’s critical assets and infrastructure from physical and cyber threats.

You Will Learn:
➤ Latest trends in nation-state hacking
➤ What (and who) is being targeted
➤ Effective and practical countermeasures

Insider Threat: Defending Against The Next Snowden
Steven Bay, Dir. of Threat Intelligence, Security On-Demand

Steven Bay, a former defense contractor, knows a thing or two about insider threats. For a time, he was the boss of Edward Snowden, the infamous leaker who stole highly classified information from the National Security Agency. In this presentation you will hear the inside story of the Snowden affair from his former boss and the lessons we learn from it. You will develop a better understanding of who insiders are, why they do what they do, and strategies you can deploy to better protect yourself from them.

You Will Learn:
➤ Strategies for spotting insider threats
➤ Lessons learned in a post-Snowden world
➤ Best practices for insider threat mitigation
➤ How to detect malicious insiders

New DCSA’s Expanded Mission & Priorities for 2020
Charles Phelan, Director, Defense Counterintelligence and Security Agency

The Defense Counterintelligence and Security Agency is now responsible for conducting 95% of the government’s background investigations. Along with its new name and expanded mission, DCSA is also rolling out improvements to the security clearance process; refining internal operations and IT systems; changing how it evaluates defense contractor security programs; updating requirements to better secure defense technology; adopting a risk-based approach to security; and much more. Find out what’s in store for DCSA (and FSOs) in 2020 and how it will impact your security program.

You Will Learn:
➤ New security requirements in the pipeline
➤ Transitioning to Tailored Security Plans
➤ Security policy changes and impacts

“I look forward to attending the Impact seminar every year. As an FSO, the topics, speakers and workshops provide invaluable information that helps me do my job better.”
Jeff Caddy
MarkLogic Corp.
**Track 1 — Cybersecurity Essentials for FSOs**  
*Robby Ann Carter, CEO*  
*SASSI/NSTI*

In the modern workplace, there are many challenges that security teams need to be prepared for — whether it’s phishing, BYOD, IoT, the list is long. Complicating matters? The growing use of unauthorized apps and the added obstacle of Shadow IT. While today’s workforce is increasingly technology savvy, their understanding of the risks they introduce has not kept pace. Keeping your organization safe from cyber risk is everyone’s job, not just the IT Department.

**You Will Learn:**
- How to identify and mitigate the risk of Shadow IT
- Actionable recommendations to address vulnerabilities
- Cybersecurity awareness best practices

---

**Track 2 — NISPPAC: Hot Button Issues For 2020**  
*Heather Sims, NISPPAC Industry Spokesperson*  
*General Dynamics, CHQ*

The National Industrial Security Program Policy Advisory Committee (NISPPAC), comprised of both Government and industry representatives, is responsible for recommending changes in industrial security policy. The group also advises the Information Security Oversight Office on all matters related to the National Industrial Security Program (NISP). In 2020 they’ll be working to create a new path forward on a number of security fronts. Attend this workshop to find out what’s on the NISPPAC agenda and how you can help shape the future of the NISP.

**You Will Learn:**
- Security policy changes on their radar
- Risk based industrial security oversight
- Industry engagement and top issues

---

**Track 1 — Roadmap: Risk Management Framework and eMASS**  
*Karl Hellmann, Asst. Dep. Director*  
*NISP Authorization Office, DCSA*

DCSA has adopted the NIST Risk Management Framework (RMF) standards as a common set of guidelines for the assessment and authorization of information systems to support contractors processing classified information. Information systems must be authorized prior to processing classified information. All requests for authorizations or reauthorization must be submitted through eMASS. This workshop will take you through the various steps to IS authorization and security plan approval. Navigating the RMF process can be confusing so come prepared to learn.

**You Will Learn:**
- Comprehensive RMF process walk through
- How to complete required eMASS tasks
- Key missteps to avoid

---

**Track 2 — Improving Security Awareness Using Marketing Techniques**  
*Mitch Lawrence, CEO, Lawrence Solutions LLC*

Security awareness and training is a critical element in the security practitioner’s toolbox that helps organizations respond better to security threats and prevent security robbing behaviors. With just a few adjustments to how your organization plans, creates and manages awareness activities, it can build awareness campaigns that are more engaging and perform better. By adapting the techniques that marketing teams use to gauge their brand awareness and interactions with potential customers, your company or agency can get increased buy-in from employees and maximize your security awareness results.

**You Will Learn:**
- Ways to increase security motivation
- How to create effective messaging
- Key marketing techniques you can leverage
Heading into 2020, we should expect nation-state actors to continue their multi-pronged espionage efforts against the United States. The FBI has over a 1,000 open cases of attempted theft of U.S. intellectual property, across a range of industries and spanning its 56 field offices around the country. U.S. intelligence officials warn that the foreign spying threat is increasing in both scale and sophistication. Every day, U.S. government and defense contractors are targeted by hostile nations 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:
- Paradigm shift in the threat landscape
- Whole-of-society approach to counter threats
- Spy tactics and exploitation methods
The United States is now facing the most significant foreign intelligence threat it has ever encountered. Adversaries are successfully attacking cleared industry at an unprecedented rate, according to the Defense Counterintelligence and Security Agency. To counter this threat, DCSA is partnering with U.S. industry to design, develop, and pilot an intelligence-led, asset-focused, and threat-driven approach to industrial security called Risk-based Industrial Security Oversight, or RISO. Defense industry partners working on critical technologies have or will undergo the RISO Comprehensive Security Review (CSR), which results in a Tailored Security Plan.

**You Will Learn:**
- Actions you can take now to prepare
- Key elements of a Tailored Security Plan
- Strategies to protect critical assets

DCSA’s vision to change the way it oversees industrial security is being ramped up for 2020. The agency wants to move from a compliance-based “check the box” inspection mentality to one that prioritizes cleared industry’s most important technology first. The agency is implementing a new methodology that is based on knowing the assets at each facility, analyzing threats to those assets, identifying vulnerabilities, and applying appropriate countermeasures. This new methodology couples NISPOM compliance with an intelligence-led, asset-focused, and threat-driven approach. Keeping up with changing requirements is critical to avoid security compliance issues and safeguard classified information.

**You Will Learn:**
- Strategies for keeping your program in compliance
- Industrial security program oversight priorities
- New Security Rating Score model

Because there are fewer controls over Controlled Unclassified Information (CUI) as compared to classified information, CUI is the path of least resistance for adversaries. Loss of aggregated CUI is the one of the most significant risks to national security, directly affecting the protection and lethality of our warfighters. As a starting point for CUI oversight, DoD has elected to begin conducting assessments of major defense contractors that are contractually obligated to protect this information. Learn about the CUI program, how it impacts you, and the steps you can take to be prepared for implementation in your organization.

**You Will Learn:**
- Key elements of the CUI program
- Update on agency implementation efforts
- CUI best practices
Defending Against Growing Cyber Threats to Classified Networks
Clint McKay, Technical Dir., NSA’s Information Assurance Directorate

Cyber threats against classified Pentagon and defense industry computers are increasing in frequency, sophistication and impact, opening up to attack vast amounts of critical data that is housed on government IT systems. These threats often pose a greater threat than physical attacks on our nation and are incredibly difficult to identify. Each day, the Department of Defense, which protects our national security and terabytes of some of the country’s most sensitive data, thwarts 36 million email breach attempts. With new threats every day and criminals who regularly diversify their attacks, experts predict cyberattacks will get worse before getting better.

You Will Learn:
- Top cyber threats for 2020
- How adversaries are targeting defense networks
- Intelligence sharing initiatives

Threats to U.S. Supply Chain and New Cybersecurity Certification
* William Stephens, Director Counterintelligence, DCSA
* Stacy Bostjanick, Director, CMMC Policy, OUSD (A&S)

Supply chains have become the gift that keeps on giving for cyber spies and information thieves. Experts estimate losses of about $600 billion per year in the transfer of wealth, expertise and trade secrets. Adversaries and bad actors specifically target the defense industrial base, using the pilfered data to close capability gaps with the United States. A new DoD initiative aims to protect critical technology from cradle-to-grave by establishing security as the foundation of the acquisition process. The Pentagon is rolling out the Cybersecurity Maturity Model Certification (CMMC) program to better protect unclassified defense data and networks.

You Will Learn:
- Why supply chain risk belongs on your radar
- All DoD contractors will require security certification

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

The National Industrial Security Program is undergoing significant changes in several key areas that will dictate future requirements for the protection of classified and controlled 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:
- CUI: Key implementation challenges
- NISPOM policy revisions and updates
- Agency self-inspection report highlights

Leadership Through Security: The Changing Role of the FSO
Evan Lesser, Co-Founder & Managing Dir., Clearancejobs.com

“Change is the only constant”—This time-worn phrase has special significance for security professionals in the National Industrial Security Program. We all know our role as FSO is constantly morphing as sweeping policy changes and technological advances now require us to wear many hats. The problem is these hats aren’t necessarily the ones we want to wear, or signed up to wear. But to be successful in the new decade, FSOs must evolve into advisors, educators and business enablers who can communicate the value of security to both management and employees. This session will show you how to adapt and thrive in this new environment.

You Will Learn:
- FSOs new playbook for 2020
- Best practices to become an effective leader
- New tools you must add to your arsenal

“Very professional! One of the better seminars I have attended. Presenters, materials, facilities all excellent.”
Michael Alvarez
Naval Special Warfare Command
Tuesday, April 21
7:00 — 7:50 am. Coffee and Pastry
7:50 — 8:00 am. Opening Remarks
8:00 — 8:45 am. Defending Against Economic Espionage In 2020 and Beyond
Senior Official, FBI, National Security Branch
8:45 — 9:30 am. Countering Terrorism in the 2020s: Examining the Evolving Threat
TBA
9:30 — 10:30 am. Managing the Human Side of Cyber Security
Shayla Treadwell, Dir., Cybersecurity-Organizational Psychologist, ESC Federal
10:30 — 11:50 am. Future of Security Clearance Vetting, Adjudication & Appeals
Tricia Stokes, Dir. of Defense Vetting, DCSA and Perry Russell-Hunter, Director, DOHA
12:00 — 1:30 pm. Host Networking Luncheon
1:30 — 2:45 pm. Track 1 – Keys to Creating a Risk-Based, Tailored Security Plan
Karl Hellmann, Asst. Dep. Director, NISP Authorization Office, DCSA
Track 2 – Personnel Clearance Innovation: The VROC & CAF
Heather Green, Dir., VROC, DCSA Vetting Directorate
Marianne Martineau, Director, DoD CAF
2:45 — 3:05 pm. Refreshment/Networking Break
3:05 — 4:20 pm. Track 1 – DCSA Industrial Security Program Issues and Answers
Gen E. Green, Dir., Industrial Security, Defense Counterintelligence and Security Agency
Track 2 – Solution for Implementing CUI Requirements
Devin Casey, Program Analyst, Information Security Oversight Office

Wednesday, April 22
7:00 — 7:50 am. Coffee and Pastry
7:50 — 8:00 am. Opening Remarks
8:00 — 8:45 am. Defending Against Growing Cyber Threats to Classified Networks
Clint McKay, Technical Dir., NSA’s Information Assurance Directorate
8:45 — 9:45 am. Threats to U.S. Supply Chain and New Cybersecurity Certification
*William Stephens, Dir. Counterintelligence, DCSA
*Stacy Bostjanick, Director, CMMC Policy, OUSD
9:45 — 10:05 am. Refreshment/Networking Break
10:05 — 10:50 am. Annual State of the National Industrial Security Program
Mark Bradley, Director, Information Security Oversight Office
Evan Lesser, Co-Founder & Managing Dir., Clearancejobs.com
11:35 — 11:45 am. Closing Remarks
Seminar Hours

Monday, April 20
Registration 7:00 am. – 7:50 am.
Conference 7:50 am. – 4:50 pm.
Networking Reception 5:00 pm. – 6:30 pm.

Tuesday, April 21
Conference 7:50 am. – 4:20 pm.

Wednesday, April 22
Conference 7:50 am. – 11:45 am.

Pre-Conference Workshop
Sunday, April 19,  2:00 pm. – 5:00 pm.

Security Awareness Fair and Expo
Monday, April 20,  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/go/NationalSecurityInstituteMTG. When calling, please ask for the NSI IMPACT 2020 rate at the Westfields Marriott in order to receive the discounted group rate of $244. The group rate will be available until March 21st 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 produce the industry’s most respected and cost-effective security awareness services. We also offer government and industry security professionals a FREE e-newsletter, delivering national and international news pertinent to the security profession. Visit us at http://nsi.org.
Who Should Attend IMPACT 2020…
- 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 Managers
- 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 __________________________

Platinum Sponsor

Gold Sponsors

Registration Fees

<table>
<thead>
<tr>
<th>Registration</th>
<th>Rcvd. by 3/2/20</th>
<th>After 3/2/20</th>
</tr>
</thead>
<tbody>
<tr>
<td>3-day Registration</td>
<td>$945</td>
<td>$995</td>
</tr>
<tr>
<td>2-day Registration</td>
<td>$895</td>
<td>$895</td>
</tr>
<tr>
<td>1-day Registration</td>
<td>$645</td>
<td>$645</td>
</tr>
</tbody>
</table>

Enroll me in the Defense Information System for Security (DISS) Workshop
Sunday, April 19, 2:00 - 5:00 pm
Note: This complimentary workshop is available to all three-day Impact registrants.
Why IMPACT 2020 Will be Your Most Critical Professional Experience of the Year

➢ 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 three 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!