National Security Institute's 36th Annual Security Forum

# IMPACT 2023

*April 17 – 19, 2023*
*Westfields Marriott • Chantilly, VA*

National Security Institute

# Rethinking Security: New Rules New Tools

**New for 2023. . .**

- **China's Growing Threat to U.S. Defense Secrets**
- **What You Need to Know About CMMC and CUI**
- **Transitioning to NBIS and Trusted Workforce 2.0**
- **Cyber Risk: What FSOs Need to Know**

# GAIN KNOWLEDGE, INSIGHTS AND EXPERTISE

## Redefining Security: New Rules, New Tools

**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 Trusted Workforce 2.0 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 2023. Join the best minds in government and industry security for three innovative days at NSI's 36th Annual IMPACT '23 Conference and Expo on April 17-19 at the Westfields Marriott in Chantilly, VA.

## Get Ready to Take Your Security Program to the Next Level

Learn everything you need-to-know from over 27 leading government and industry security experts at IMPACT '23 — the one conference you and your security team can't afford to miss this year.

Led by a top-flight faculty of speakers and trainers, IMPACT '23 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 NBIS Bonus Workshop

Pre-Conference NBIS Training
Sunday, April 16, 2:00 pm — 5:00 pm

This three-hour complimentary workshop will help you successfully navigate the transition to the National Background Investigation Services platform. This bonus workshop is available to three-day registrants only.

*"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*

## 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.

# IMPACT 2023 EXTRAS!

## 5 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 2023.

### 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; 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 2023 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 2023 Exhibitors

DMP
SIMS SOFTWARE
MATHCRAFT SECURITY TECHNOLOGIES, INC
NSA
SECURITY CONTROL
Sign In Compliance formerly ThreatSwitch
NSTI
ALPHASAFE
Securitas
FBI
DCSA
WHITAKER BROTHERS
TALKEN INDUSTRIES
SECURESTRUX

## Valuable Take-Home Resources

Every IMPACT '23 registrant goes home with a comprehensive binder of seminar materials and handouts and access to the 2023 Edition of NSI's Reference Library.

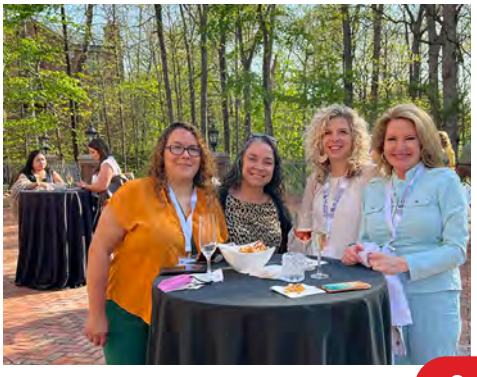

This remarkable resourse is packed with articles, white papers, checklists, glossaries, reports, surveys, and primary sources.

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 17, 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.

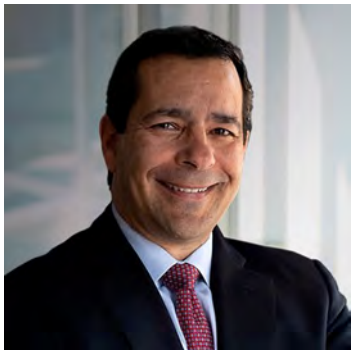


# Monday April 17

# EDUCATIONAL SESSIONS

## Keynote Address:

*Monday, April 17 8:00am-8:45am*



### National Security Threats: Confronting a New World of Risk

*William Evanina, CEO, The Evanina Group and Former Director, NCSC*

The foreign intelligence threat to the nation's defense industrial base has never been more capable, sophisticated, or complex. Adversaries use illicit methods to acquire classified and sensitive information and technologies, which can determine the outcome of future conflicts. From nation-state espionage to cyberattacks and insider threats, the security risks we face as a nation have never been greater or more diverse. Mitigating these threats starts with understanding them. 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 2023 and how to safeguard your organization's critical information

*Monday, April 17 8:45am-9:30am*

### Understanding the Increasing Threat Of Nation-State Cyber Attacks

*Neil Ziring, NSA Cybersecurity Collaboration Center*

There has been a disturbing increase in the number of nation-state cyber attacks directed at government and defense industry networks. These attacks 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. Cybersecurity is a team sport and NSA has established a new Cybersecurity Collaboration Center to assist defense industry stakeholders in identifying emerging threats and implementing defensive measures to protect critical U.S. technology secrets.

**You Will Learn:**

- Latest trends in nation-state hacking
- What (and who) is being targeted
- Effective and practical countermeasures

*Monday, April 17 10:30am-11:45am*

### Why (and How) FSOs Should Create a Culture of Collaboration

*David Tender, Sr. VP,CSO, ASRC Federal; Mary Rose McCaffrey, VP Security, Northrup Grumman; Charles Phalen, C.S. Phalen & Associates; James Kennedy, CSO, MIT Lincoln Laboratory*

Today's FSO is seated closer to the executive function than ever before, and tasked with educating their Senior Management Official (SMO) as well as other key department heads regarding security threats to people, processes and technology. Getting top management and security on the same page is a critical component of a robust security posture. To sell the value of our contribution to the company's senior management, FSOs must be able to market their role more strategically and collaborate with key partners in HR, IT and Legal to respond faster to security threats, reduce risk and improve resilience. Simple shifts in security mindset and behaviors can have an outsized effect on the speed and effectiveness of collaboration in your organization. If you're looking for a lever, look no further. You are it.

*Monday, April 17 11:45am-12:45pm*

### DCSA 2023: Security Transformation In the Digital Age

*William Lietzau, Director, Defense Counterintelligence and Security Agency*

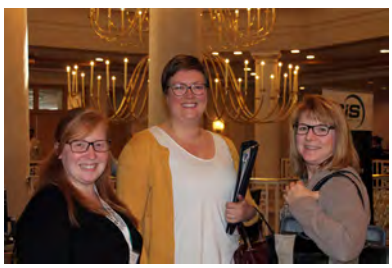
The Defense Counterintelligence and Security Agency continues its transformation as it works to impact national security with the most effective and technologically advanced personnel vetting, background investigations, adjudications, counterintelligence, counter insider threat, industrial security, and educational products. Reducing costs and improving investigation quality has been a key goal even before DCSA took over the background investigations process from NBIB in 2019. The agency continues to roll out these and other improvements to their internal operations and IT systems and refining how it evaluates defense contractor security programs. Find out what's in store for DCSA (and FSOs) in 2023 and how it will impact your security program.

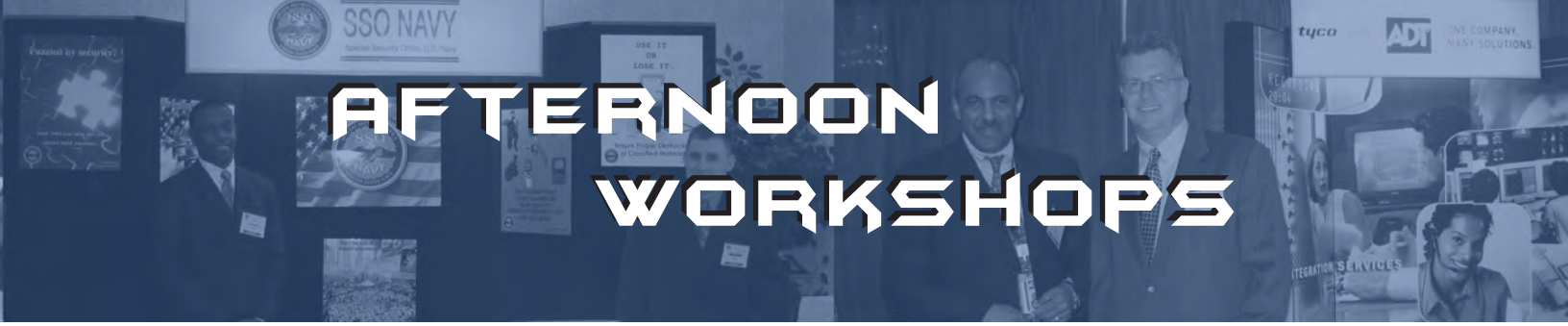
**You Will Learn:**

- Industry onboarding to NBIS
- Implementation of Trusted Workforce 2.0

*"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.*






# AFTERNOON WORKSHOPS

*Monday, April 17 2:00pm-3:15pm*

## Track 1 — Cybersecurity Essentials for FSOs

*Dr. Shawn P. Murray, CCISO, CISSP, CRISC*
*President, CAO, Murray Security Services*

In today's landscape of escalating cybercrime, mitigating cyber risk is not the IT department's responsibility alone—it is everyone's job. Getting ahead of hackers and other security risks requires the active engagement of non-technical management, as well as an overall commitment to building a cybersecurity culture within your enterprise. Effectively managing risk begins with a baseline understanding of today's cyber threats. This workshop will provide you with advanced understanding and skills to protect your organization's critical information against the most common cyber threats.

**You Will Learn:**

- Understand key terms and concepts in cyber security
- Build key skills to recognize common security threats
- Take steps toward creating a strong security culture

*Monday, April 17 2:00pm-3:15pm*

## Track 2 — Best Practices in Implementing Your Insider Threat Program

*Kevin Clifton, Head of Intelligence and Risk Management, RAND Corporation*
*Mark Levett, Director, Corporate Security, Cyber Intelligence, L3Harris Tech*
*Mark Werkema, Strategic Intelligence, Boeing Company*

Insider Threat Programs are designed to deter, detect, and mitigate actions by insiders who represent a threat to national security. Now that you've met the baseline requirements, how does your insider threat program measure up against the best-in-class? Effective insider threat programs need more than just a great security team – they also need collaboration across a multitude of teams. Successful insider threat programs rely on teamwork across levels and functions. Join this session to hear from key defense industry experts as to how they built and operationalized their program.

**You Will Learn:**

- Getting buy-in from the organization
- Examples of positive security outcomes
- Steps to create an efficient insider threat program

*Monday, April 17 3:35pm-4:50pm*

## Track 1 — RMF and eMASS: Keys to Getting Your Systems Approved

*David Scott, NISP Authorizing Official, 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

*Monday, April 17 3:35pm-4:50pm*

## Track 2 — How to Take Your Awareness Program from 'Good' to Great

*Roslyn Wesley, Sr. Mgr. Audit & Compliance, MIT Lincoln Lab*
*Jeremy Treadwell, Co-Founder, Mgr. Dir., Treadwell Agency*

Protecting your most sensitive data takes more than just the right security tools—it takes a well-structured security awareness & education program with a simple strategy for getting people's attention and increased cooperation. Every incremental step towards a great SETA program is a step towards increased risk mitigation and stronger protection of your organization's classified data and CUI. Learn new methods that motivate employees to integrate security thinking into their everyday routine. Get ideas you can use right away, ways of thinking about how to actually reach people and get them on your side, and a simple method for planning out a proven-effective program you can scale over time.

**You Will Learn:**

- Easy way to apply a "marketing plan" structure
- Account for different learning styles, ages, roles
- Tips for being creative and persuasive

# Tuesday April 18

# EDUCATIONAL SESSIONS

*Tuesday, April 18 8:00am-8:45am*

## Trends in Terrorism: What's on the Horizon in 2023

*Abby Johnson, Deputy Director*
*National Counterterrorism Center*

Despite significant progress in diminishing the terrorist threat to the United States, the country continues to face a diversified, transnational, and in many ways unpredictable threat environment both at home and abroad. An array of actors, whether foreign terrorist organizations, state sponsors of terrorism, or lone actors, are shaping the nature of today's terrorism landscape. Against the backdrop of this threat landscape, whether overseas or at home, NCTC remains focused on uncovering and disrupting transnational networks from which threats to Americans and America are likely to emerge. This session will examine the latest threats, explore emerging trends and future forecast.

**You Will Learn:**

- Paradigm shift in the threat landscape
- New initiatives in the fight against terrorism
- Counterterrorism strategies and tactics

*Tuesday, April 18 8:45am-9:45am*

## Deep Dive: Understanding the Growing China Threat

*Nicholas Eftimiades, Asst. Teaching Professor, Penn State University*

America received a wake-up call recently when China flew a spy balloon across the United States. But if the vehicle for espionage seemed novel, the concept was anything but. China has aggressively been targeting U.S. industry and government agencies with espionage operations designed to collect troves of sensitive and classified information for years. In fact, FBI Director Christopher Wray warned that China espionage is the greatest threat to the U.S. and its allies. China uses a wide array of methods to steal the U.S. government's most sensitive secrets. Understanding the Chinese espionage threat better will help us respond to it more effectively.

**You Will Learn:**

- China's Intel Ops and tactics against the West
- China's whole-of-society approach

*Tuesday, April 18 10:05am-10:50am*

## DoD Policy Trends Shaping Security in 2023

*David Tender, Industry Member*
*NISPPAC*

The National Industrial Security Program is undergoing significant changes in several key areas that will dictate future requirements for personnel security and the protection of classified and controlled unclassified information. The NISPPAC, comprised of both Government and industry representatives, is at the forefront for recommending needed changes in industrial security policy. The NISPPAC also advises the government's Information Security Oversight Office on all matters concerning the policies of the National Industrial Security Program. Learn about the current strategic industry NISP priorities that will shape security policies for years to come.

**You Will Learn:**

- Security reforms and Trusted Workforce 2.0
- CUI and CMMC
- Industry engagement and key issues

*Tuesday, April 18 10:50am-11:50pm*

## How to Avoid Clearance Problems, Denials and Revocations

*Perry Russell-Hunter, Director*
*DOHA*

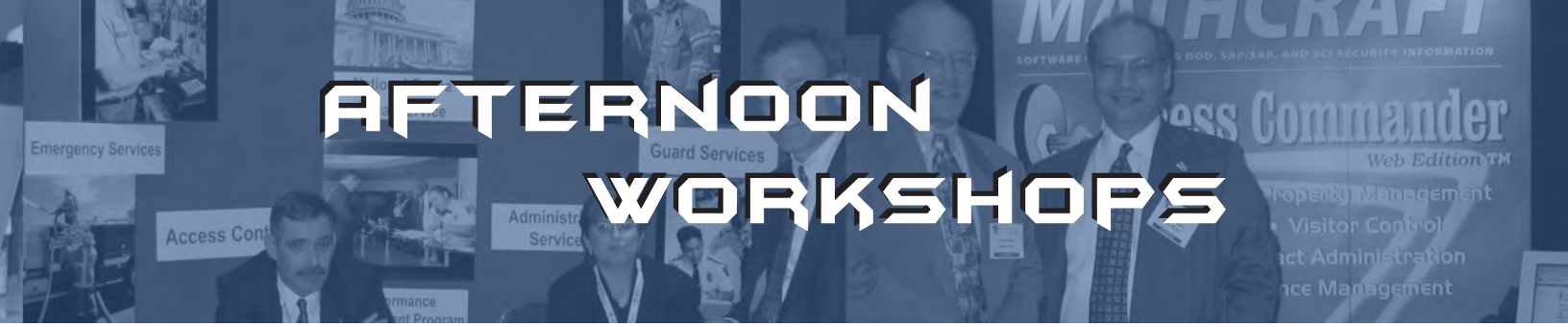
The Defense Office of Hearings and Appeals (DOHA) conducts industrial security clearance reviews for defense contractor employees who appeal the denial or revocation of a security clearance. While the majority of applicants are granted a clearance, complicating factors may delay a decision or result in a denial or revocation of a security clearance. Financial and criminal issues continue to be the top reason for clearance denial or revocation. And with the general adoption of Continuous Vetting (CV), the Government is finding adverse information much sooner than it would otherwise. This session will examine where clearance and investigative reforms are headed and how it impacts your organization.

**You Will Learn:**

- Trends in adjudications and appeals
- Whole-person trust determination
- Initiative to issue conditional clearances

*"This was my first time attending an Impact seminar. I obtained information in which I would not have access to otherwise. I look forward to attending again."*

*Latoya Rose, ANSER*




# AFTERNOON WORKSHOPS

*Tuesday, April 18 1:30pm-2:45pm Track 1*

## Track 1 — DCSA Industrial Security Program Issues and Answers

*Gus Greene, Director, Industrial Security Directorate, DCSA*

As the national security risk landscape changes and threat vectors continue to evolve, DCSA has transitioned from a compliance-based "check the box" inspection mentality to one that prioritizes cleared industry's most important technology first. Under the new protocol, cleared contractors will first be evaluated for general conformity to identify any critical vulnerabilities, with a focus on the company's security policies, systemic vulnerabilities (e.g., deficiencies in several different areas) or serious security issues. Last year, DCSA conducted more than 2,300 formal security reviews and 1,700 hybrid security monitoring actions. This informative Q&A session gives you a heads up on what problem areas IS reps are finding and will help you build a Cogswell-worthy security program.

**You Will Learn:**

- Strategies for keeping your program deficiency-free
- Optimize security rating score model
- Industrial Security Program oversight priorities

*Tuesday, April 18 1:30pm-2:45pm Track 2*

## Track 2 — The 5 Must-Have Critical Thinking Skills for Today's Security Professional

*Kathy Pherson, CEO, Pherson Associates*

In addition to meeting NISPOM standards, today's FSO is increasingly being leaned on to bring solutions that work for their business partners while protecting not only what's classified, but everything with high value. The successful FSO is one recognized as a strong business partner able assess difficult problems, anticipate the unexpected, develop creative solutions and avoid disastrous mistakes. In this session you will learn the critical thinking techniques that empower you to persuasively frame up and drive solutions for any operational or strategic challenge you face as a security professional: how to deal with ambiguity from regulators, positioning security priorities to win support, scaling programs methodically, dealing with limited resources – any challenge you face as a security professional.

**You Will Learn:**

- Techniques for taking control of any challenge
- Ensure your business partners are on the same page as you
- Deal with inconsistencies, ambiguity and shifting priorities

*Tuesday, April 18 3:05pm–4:20pm Track 1*

## Track 1 — Transitioning to NBIS and TW 2.0

*Jeffrey Smith, Exec. Dir., NBIS, DCSA*
*Heather Green, Asst. Dir., VRO, DCSA*
*Marianna Martineau, Asst. Dir., CAS, DCSA*

Cleared defense contractors are in the process of onboarding into the National Background Investigation Services (NBIS) — a unified personnel vetting platform comprising background investigations, adjudications and continuous vetting. This database will be accessible by adjudicators (in DCSA's Consolidated Adjudicative Services), continuous vetting analysts, and industry FSOs submitting cases through the NBIS central repository. NBIS is the backbone of the Trusted Workforce 2.0 whole-of-government background investigation reform effort overhauling the personnel vetting process. Continuous vetting within TW 2.0 will fully replace periodic reinvestigations by employing a full suite of automated record checks.

**You Will Learn:**

- NBIS deployment plan and timeline
- Future transition from e-QIP
- Industry collaboration essential to NBIS success

*Tuesday, April 18 3:05pm–4:20pm Track 2*

## Track 2 — Counterintelligence Lessons from Key Espionage Cases

*Peter J. Lapp, President, PJ Lapp Consulting, LLC*

The United States is losing the counterintelligence war. Foreign intelligence services, particularly those of China, Russia, and Cuba, are recruiting spies in our midst and stealing our secrets and cutting-edge technologies. Ana Montes was the consummate insider threat who went undetected for years. Unlike the FBI's Robert Hanssen or the CIA's Aldrich Ames, Montes took no money for the secrets she gave to the Cubans.This timely workshop analyzes valuable lessons learned from significant counterintelligence case studies, including espionage motivation, characteristics of spies, and successes and failures of various security measures. You'll leave better prepared to counter the growing espionage challenge.

**You Will Learn:**

- Effective CI strategies and techniques
- Why trusted insiders spy
- How to avoid becoming a soft target

# Wednesday April 19

# EDUCATIONAL SESSIONS

*Wednesday, April 19 8:00am-8:45am*

## Counterintelligence: Defending U.S. Technology Secrets

*Allen E. Kohler Jr., FBI Asst. Director, CI Division*

Every day, U.S. government and defense contractors are targeted by hostile nations for espionage and theft of intellectual property, resulting in huge losses of national security information and technology secrets. These adversaries use traditional intelligence tradecraft against vulnerable American companies, and they increasingly view the cyber environment—where nearly all-important business and technology information now resides—as a fast, efficient, and safe way to penetrate the foundations of our economy. U.S. intelligence officials warn that the foreign spying threat is increasing in both scale and sophistication. Staying ahead of the threat requires constant vigilance.

**You Will Learn:**

- Spy tactics and exploitation methods
- How adversaries are targeting DIB
- Key defensive measures

*Wednesday, April 19 8:45am-9:45am*

## What You Need to Know About CMMC and CUI

*Stacy Bostjanick, Dir. of CMMC Policy, DoD ; Booker Bland, Dep. Sr. Policy Advisor, DCSA*

CMMC 2.0 will soon be the law of the land. Are you ready? Companies bidding for defense contracts will have to comply with revised Cybersecurity Maturity Model Certification requirements by the end of fiscal year 2023. The time to begin compliance planning is now. The CMMC program is a comprehensive framework to protect the Defense Industrial Base from increasingly frequent and complex cyberattacks from hackers and unfriendly nation-states. It was developed to systematically assess and certify the maturity of an organization's cybersecurity processes and procedures. Get ahead of the curve on the CMMC 2.0 and CUI, so you are best positioned to help your company meet this requirement.

**You Will Learn:**

- How to successfully navigate CMMC 2.0
- Step by step guide on certification
- Safeguarding Controlled, Unclassified Info

*Wednesday, April 19 10:05am-10:50am*

## Mitigating Unintentional 'Friendly Fire' Insider Threats

*Dr. Shayla Treadwell, VP of Governance, Risk and Compliance, ECS*

People who commit cyber friendly fire don't do so with malicious intent. Even the best employees can expose your organization to threats through carelessness or negligence. Users are human and threat actors take advantage of poor security habits and cultures. Building a positive security culture goes a long way to ensuring that employees will become part of the solution rather than the problem. That's why more organizations are shifting their mindset around security and adopting a people-centric approach to risk management. A culture of cybersecurity awareness and responsibility can help prevent some insider threats from happening and increase the likelihood that others will be caught or reported.

**You Will Learn:**

- How to build a positive security culture
- Psychology of an insider threat
- Human factors in information security

*Wednesday, April 19 10:50am-11:35am*

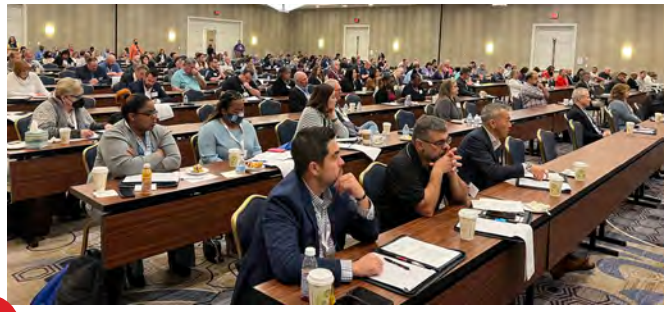
## Security and the C Suite: Bridging the Communications Gap

*Charles Sowell, CEO, SE&M Solutions LLC*

FSOs are officially getting a direct line to senior management. This elevated role is mandated by the NISPOM Rule which assigns the ultimate authority for the company's security program to the Senior Management Official or SMO. This will be someone like the president or CEO where traditionally the buck stops here. How prepared are you for this career-enhancing opportunity to engage with senior leadership on a regular basis? Step one in communication is understanding the language and priorities of the business. When communicating with the C-Suite, FSOs have to speak equal parts security and bottom line. Learn to position security as something that helps achieve organizational goals, not simply those for yourself or your team. Such positions affirm your ability to think strategically.

**You Will Learn:**

- How to brief the SMO
- Position security as a business enabler



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

*Michael Alvarez*
*Naval Special Warfare Command*

# AT-A-GLANCE
## THREE DAYS OF CAREER-CRITICAL INFORMATION


## Monday, April 17

| | |
|---|---|
| 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. | **National Security Threats: Confronting a New World of Risk**<br>William Evanina, CEO, The Evanina Group and Former Director, NCSC |
| 8:45 — 9:30 am. | **Understanding the Increasing Threat of Nation-State Cyber Attacks**<br>Representative, NSA Cybersecurity Collaboration Center |
| 9:30 — 10:30 am. | Opening of Awareness Fair, Expo and Refreshment Break |
| 10:30 — 11:45am. | **Why (and How) FSOs Should Create a Culture of Collaboration**<br>David Tender, ASRC Federal; Mary Rose McCaffrey, Northrup Grumman; Charles Phalen, C.S. Phalen & Associates; James Kennedy, MIT Lincoln Laboratory |
| 11:45 — 12:45 pm. | **DCSA 2023: Security Transformation In the Digital Age**<br>William Lietzau, Director, Defense Counterintelligence and Security Agency |
| 12:45 — 1:45 pm. | Host Networking Luncheon, Security Awareness Fair and Expo |
| 2:00 — 3:15 pm. | **Track 1 – Cybersecurity Essentials for FSOs**<br>Robby Ann Carter, CEO, SASSI/NSTI<br>**Track 2 – Best Practices in Implementing Your Insider Threat Program**<br>Kevin Clifton, RAND Corp.; Mark Levett, L3Harris Tech; Mark Werkema, Boeing |
| 3:15 — 3:35 pm. | Refreshment Break, Security Awareness Fair and Expo |
| 3:35 — 4:50 pm. | **Track 1 – RMF and eMASS: Keys to Getting Your Systems Approved**<br>David Scott, NISP Authorizing Official, DCSA<br>**Track 2 – How to Take Your Awareness Program from 'Good' to Great**<br>Roslyn Wesley, MIT Lincoln Lab; Jeremy Treadwell, Treadwell Agency |

## Tuesday, April 18

| | |
|---|---|
| 7:00 — 7:50 am. | Coffee and Pastry |
| 7:50 — 8:00 am. | Opening Remarks |
| 8:00 — 8:45 am. | **Trends in Terrorism: What's on the Horizon in 2023**<br>Abby Johnson, Deputy Director, National Counterterrorism Center |
| 8:45 — 9:45 am. | **Deep Dive: Understanding the Growing China Threat**<br>Nicholas Eftimiades, Asst. Teaching Professor, Penn State University |
| 9:45 — 10:05 am. | Refreshment/Networking Break |
| 10:05 — 10:50 am. | **DoD Policy Trends Shaping Security in 2023**<br>David Tender, Industry Member, NISPPAC |
| 10:50 — 11:50 pm. | **How to Avoid Security Clearance Problems, Denials and Revocations**<br>Perry Russell-Hunter, Director, DOHA |
| 12:20 — 1:30 pm. | Host Networking Luncheon |
| 1:30 — 2:45 pm. | **Track 1 – DCSA Industrial Security Program Issues & Answers**<br>Gus Greene, Director, Industrial Security Directorate, DCSA<br>**Track 2 – 5 Critical Thinking Skills for Today's Security Professional**<br>Kathy Pherson, CEO, Pherson Associates |
| 2:45 — 3:05 pm. | Refreshment/Networking Break |
| 3:05 — 4:20 pm. | **Track 1 – Transitioning to NBIS and TW 2.0**<br>Jeffrey Smith, Exec. Dir., NBIS, DCSA; Heather Green, Asst. Dir., VRO, DCSA; Marianna Martineau, Asst. Dir., CAS, DCSA<br>**Track 2 – Security Lessons Learned from Key Espionage Cases**<br>Peter Lapp, President, PJ Lapp Consulting, LLC |

*"Excellent Seminar. Timely topics, knowledgeable speakers and great staff."*
*Tiffaney Coleman*
*DIA*

## Wednesday, April 19

| | |
|---|---|
| 7:00 — 7:50 am. | Coffee and Pastry |
| 7:50 — 8:00 am. | Opening Remarks |
| 8:00 — 8:45 am. | **Counterintelligence: Defending U.S. Technology Secrets**<br>Allen E. Kohler Jr., FBI Asst. Director, CI Division |
| 8:45 — 9:45 am. | **What You Need to Know About CMMC and CUI**<br>Stacy Bostjanick, DoD CIO; Booker Bland, Dep. Sr. Policy Advisor, DCSA |
| 9:45 — 10:05 am. | Refreshment/Networking Break |
| 10:05 — 10:50 am. | **Mitigating Unintentional 'Friendly Fire' Insider Threats**<br>Dr. Shayla Treadwell, VP of Governance, Risk and Compliance, ECS |
| 10:50 — 11:35 am. | **Security and C Suite: Bridging the Communications Gap**<br>Charles Sowell, CEO, SE&M Solutions LLC |
| 11:35 — 11:45 am. | Closing Remarks |

# REGISTER EARLY & SAVE

## FOUR EASY WAYS TO REGISTER

1. **Register online at:** https://www.nsi.org/events/impact-2023/
2. **Fax the registration form with payment information to: (508) 507-3631**
3. **Mail the registration form and payment to:** National Security Institute
   3 Sanger Circle
   Dover, MA 02030
4. **Call (508) 533-9099**

## REGISTER NOW TO RESERVE YOUR SEAT

The full conference registration rate is $1,099, and includes the pre-conference NBIS training workshop; two-day registration is $999; and one-day registration is $799. The registration fee covers all program materials, host reception, luncheons and refreshment breaks. 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 17th will be subject to a $50 administrative fee. Cancellations received after March 17, 2023 will forfeit the conference fee. Substitutions may be made at any time by calling NSI.

### Seminar Hours

**Monday, April 17**
**Registration 7:00 am.–7:50 am.**
**Conference 7:50 am.–4:50 pm.**
**Networking Reception 5:00 pm.–6:30 pm.**
**Tuesday, April 18**
**Conference 7:50 am.–4:20 pm.**
**Wednesday, April 19**
**Conference 7:50 am.–11:45 am.**

### Security Awareness Fair and Expo

**Monday, April 17, 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 Passkey at **1-800-266-9432** or reserve your room online at https://book.passkey.com/go/607a1c96. When calling, please ask for the NSI IMPACT 2023 rate at the Westfields Marriott in order to receive the discounted group rate of $219. The group rate will be available until March 24th 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.

# REGISTRATION FORM

## Who Should Attend IMPACT 2023…

- Facility Security Officers
- Information System Security Officers
- 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 and CUI Managers
- Security Adjudicators
- Insider Threat Program Managers

**Platinum Sponsor**

Sign In Compliance
formerly ThreatSwitch

**Gold Sponsors**

MATHCRAFT SECURITY TECHNOLOGIES, INC.

Securitas

NSTI National Security Training Institute

SIMS® SOFTWARE

## Priority Registration Form

**IMPACT 2023**

**Rethinking Security: New Rules, New Tools**

Chantilly, Virginia, April 17 - 19, 2023

*Please print, type or attach your business card and forward to: National Security Institute, 3 Sanger Circle, Dover, MA 02030. Tel: 508-533-9099 Fax: 508-507-3631. Photocopy for additional registrations.*

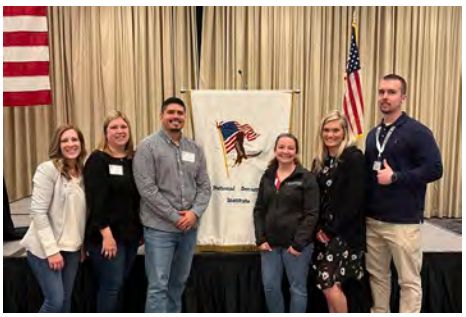
Name: _____ Title: _____

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

| | |
|---|---|
| 3-day Registration | ❑ $1,099 |
| 2-day Registration | ❑ $999 |
| 1-day Registration | ❑ $799 |

*"NSI's Impact seminar is the perfect security forum for security professionals. It does not matter if you're industry or government; junior, mid-level or C-suite. Their speakers are always first-class presenters."*

*Lucas Bosch*
*Telephonics Corporation*

National Security Institute
3 Sanger Circle
Dover, MA 02030

## Why IMPACT 2023 Will be Your Most Critical Professional Experience of the Year

- You'll get up to date on the hottest security issues: security clearances, NBIS, NISP, classified systems security, economic espionage, cyber security threats, security awareness, terrorism, CMMC and insider threats.
- You'll return to your office with an entire reference library that will put the information you need at your fingertips: binder, Resource Library, 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 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!

### 11 Special Features of IMPACT 2023

- In-depth, practical workshops, not PowerPoint snooze-a-thons!
- Briefings with important heads of government agencies
- 2023 Edition of NSI's Reference Data Library
- Sessions targeted to personal and professional development, that will help you become better at your job
- NSI's 2023 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 2023 to address the hottest security topics
- Excellent, business-class hotel, minutes from major airports
- Take-away binder of conference program materials