CDSE
LEARN. PERFORM. PROTECT.

PULSE

VOLUME 7 ISSUE 4 | April 2026

CDSE Pulse

Published by the Security Training Directorate Outreach and Engagement Office for the Center for Development of Security Excellence (CDSE).

DCSA Leadership

The Honorable Justin P. Overbaugh
Acting Director, DCSA

Tara Jones
Acting Deputy Director, DCSA

CDSE Leadership

Audrey Gutierrez
Director

Glenn Stegall
Deputy Director

Dr. Shafiah Firoz
Division Chief, DOD Security Training

Dr. Monica Minor-Exum
Division Chief, Credentialing & Certification Division

Pulse Staff

Cashmere He
Chief Content Officer

Jenise Kaliszewski
Tammi Bush
Content Contributors

Marc Pulliam
Content Designer

Center for Development of Security Excellence

CDSE – Center for Development of Security Excellence

@TheCDSE

Center for Development of Security Excellence

THIS MONTH'S FOCUS

Securing Commerce: National Supply Chain Integrity Month

By Tammi Bush

In an increasingly interconnected world, the security of our supply chains is not just a business concern; it's a matter of national security. Designated as National Supply Chain Integrity month, April is dedicated to encouraging organizations to safeguard supply chains against foreign adversaries and other potential threats. The Center for Development of Security Excellence (CDSE) contributes by educating and preparing organizations across the country to safeguard supply chains against threats through training, webinars, and other resources.

The intricate network of organizations, people, and resources that move products from supplier to customer is vital to the global economy. However, this also presents vulnerabilities that adversaries can exploit. This month focuses on strengthening systems against a growing array of threats.

A supply chain includes the entire system which moves a product or service from origin to the end user. Supply chain risk management is the systematic process of identifying, assessing, and mitigating threats within that system.

Adversaries, both foreign and domestic, actively work to disrupt these chains. The threats are diverse and can manifest at any point in the supply chain lifecycle, from design and manufacturing to

deployment and retirement. A significant concern is the rise in cargo theft, which is growing. Because adversaries exploit supply chains to target U.S. equipment, systems, and information, supply chain resilience a critical component of national security.

Recognizing the gravity of these threats, U.S. government agencies like the Cybersecurity and Infrastructure Security Agency (CISA) are championing a more resilient and secure approach. Integrating security alongside traditional risk management tenets of cost, schedule, and performance is vital and involves proactive identification and counter attacks.

CDSE is at the forefront of providing resources to combat these threats, offering a range of tools and training to educate and empower organizations to protect their supply chains.

Supply Chain Resources:

- **Supply Chain Threat Awareness Course** (CI102.16) provides a foundational understanding of supply chain threats.
- **Counterintelligence Awareness Toolkit** (Supply Chain Risk Management tab) includes a dedicated section on supply chain risk management, featuring CDSE-created content, job aids, eLearning courses, and webinars.
- **Deliver Uncompromised Supply Chain Risk Management Job Aid** outlines the risk management process.
- **Insider Threat to Supply Chains Job Aid** outlines how to recognize and protect against various cyber threats.

Additionally, several organizations offer digital media related to supply chain risk management:

- CISA's **ICT Supply Chain Resource Library** is a list of free resources and information on supply chain programs and activities from across the federal government.
- The National Counterintelligence and Security Center's **Supply Chain Management for Industry and Academia webpage** includes supply chain jobs aids, toolkits, videos, and webinars.
- Office of the Director of National Intelligence's **Know the Risk – Raise Your Shield: Supply Chain Risk Management video** focuses on supply chain integrity, and how to mitigate risks.

Supply chain integrity challenges are significant and constantly evolving. By leveraging the available resources, staying informed, and fostering a culture of security, organizations can build the resilience needed to withstand these threats. Protecting supply chains is a shared responsibility, and an essential piece to safeguarding our economy and national security.

INSIDER THREAT

Insider Threat Detection Analysis Course (ITDAC)

Sharpen your insider threat analyst skills. In just five days, CDSE's ITDAC will equip you with critical thinking skills and analytic techniques to tackle potential insider threats.

Through extensive, real-world practical exercises, this course will include how to:

- Collect and interpret holistic data.
- Apply critical pathway theory.
- Master the process for conducting and reporting response actions, from initial intake to threat mitigation.

This course is open to all federal insider threat program analysts in Executive Branch departments and agencies and satisfies the training requirements of the 2012 presidential memorandum on National Insider Threat Policy.

Visit the **ITDAC page** to register for an upcoming virtual session:

- April 13 - 17, 2026
- May 11 - 15, 2026
- June 8 - 12, 2026
- July 13 - 17, 2026

New Case Study: John Murray Rowe Jr.

Who is John Murray Rowe Jr.? A 67-year-old test engineer, Rowe is a U.S citizen who worked for several defense contractors over the span of nearly 40 years. Due to the sensitive nature of his work related to U.S. Air Force electronic warfare technology, Rowe was granted access to national defense information, holding clearances from secret to top-secret/sensitive compartmented information (TS/SCI).

In 2017, a Facility Security Officer (FSO) identified Rowe as a potential insider threat based on review of his online social media profile and social media posts he made.

Following a 2021 arrest, Rowe pleaded guilty to one count of attempted delivery of national defense information to a foreign government and three counts of willful communication of national defense information. On Sept. 15, 2025, Rowe was sentenced to 126 months in prison, three years of supervised release, and a $25,000 fine.

Learn more about the crime, the sentence, the impact, and the potential risk indicators that, if identified, could have mitigated harm. Access the **case study** to review this case.

INFORMATION SECURITY

Activity Security Manager for InfoSec Course (IF203.10)

Information is a strategic asset, vital to our national security. Learn how to protect it effectively in the virtual "**Activity Security Manager for InfoSec**" course from April 19 to May 17.

In this four-week, mid-level course, participants will develop the expertise to mitigate risks and master the implementation and evaluation of a robust Information Security Program (ISP). This training is ideal for civilian, military, or contractor personnel responsible for managing an ISP.

Elevate your security management skills and ensure you are mission ready. Secure your spot today!

INDUSTRIAL SECURITY

Getting Started Seminar for New Facility Security Officers (IS121.10)

Stepping into a new security role? Get the foundational knowledge you need to excel with the virtual "Getting Started Seminar for New Facility Security Officers (FSO)" course.

This seminar is the perfect opportunity to familiarize yourself with critical NISP requirements in a dynamic and collaborative group setting. It is specifically designed to support new FSOs, contractor security personnel, DOD Industrial Security Specialists, and any other professionals navigating the security landscape.

Virtual classes are offered on the following dates:

- May 12 - 15, 2026
- July 21 - 24, 2026

In-Person NCMS Annual Training Seminar Opportunity:

CDSE will also host the Getting Started Seminar (GSS) for Facility Security Officers (FSOs) at the NCMS Annual Training Seminar on June 8, 2026!

This course is not only a great way to get started as a new FSO, but also a way for experienced FSOs to keep informed on industrial security guidance and emerging trends. Students will work in collaboration with other security professionals, exploring security topics through practical exercises. Topics include the DD 254, insider threat, reporting requirements, counterintelligence, security and contractor reviews, security training and briefings, and personnel security.

Please **register** and complete the pre-requisites **here**. Registration closes on May 15, 2026, and only fully registered participants will be allowed to attend. You will receive registration confirmation via email directly from CDSE and must bring proof of this CDSE email confirming GSS registration as well as a photo ID for class entry on June 8th. You must also be registered for the NCMS Annual Training Seminar to attend the GSS. You will not be fully registered for the GSS until you complete the pre-requisites and submit attestation of NCMS registration in STEPP. ***Please note that absolutely no walk-ins will be allowed***. The GSS is free, and fills up fast, so register today!

GENERAL SECURITY

DOD Security Specialist Course (VILT GS101.10)

Finding time for professional development can be a challenge. That's why CDSE has designed a training solution to fit your busy schedule.

Join CDSE's virtual "DOD Security Specialist Course" from **April 6 to May 3**. This flexible, four-week online program allows you to master fundamental security tasks and practices in just a few hours each day. Participants will receive the same expert instruction and comprehensive content as the in-person course.

Invest in your growth and find a session that suits your schedule. **Sign up today**!

CYBERSECURITY

Instructor-Led Training: Assessing Risk and Applying Security Controls to National Industrial Security Program (NISP) Systems (CS301.01)

The cybersecurity team is excited to announce a new training opportunity: "**Assessing Risk and Applying Security Controls to NISP Systems**."

This in-depth course provides critical guidance on applying policies to protect information within the Risk Management Framework (RMF) and offers a comprehensive review of contractor requirements under the NISP.

This training is highly recommended for:

- Information System Security Managers (ISSM)
- Information System Security Officers (ISSO)
- Facility Security Officers (FSO)
- Personnel involved in the planning, management, and execution of security programs for cleared industry.

In-person sessions will be held in Linthicum, Md., on the following dates:

- May 4 - 8, 2026
- Aug. 17 - 21, 2026

Register **here** via STEPP.

PERSONNEL VETTING

Fundamentals of National Security Adjudications VILT (PS101.10)

Are you prepared to take on a vital role in the protection of our nation's secrets? Join fellow security professionals from April 20 - 28 for CDSE's virtual course, "Fundamentals of National Security Adjudications." Gain the essential skills to identify security concerns and make crucial personnel security determinations.

Register to secure your spot today.

BEHAVIORAL THREAT ANALYSIS CENTER

BTAC Bulletin

Stay informed about evolving threats with the latest edition of the Behavioral Threat Analysis Center (BTAC) Bulletin.

The monthly **bulletin** is a go-to resource for relevant insider threat guidance. The bulletin is crafted by a multidisciplinary team of experts in threat assessment and management, law enforcement, counterintelligence, behavioral science, employee management relations, and cybersecurity.

View the latest BTAC Bulletin today and empower your team with the knowledge to identify, mitigate, and manage insider risks effectively.

PHYSICAL SECURITY

Physical Security and Asset Protection (PY201.01)

Join the "Physical Security and Asset Protection" (PY201.01) course May 11 - 15, 2026, in Linthicum, Md. This course teaches students to identify and utilize regulatory guidance, methodologies, and concepts for protecting DOD assets. Students will be able to apply the risk management process, conduct problem solving, and incorporate best practices to develop courses of action utilizing physical security measures, based on a cost-benefit analysis, to protect an installation's assets. **Register** today!

SPECIAL ACCESS PROGRAMS

Special Access Programs Courses

"Introduction to Special Access Programs (SAP)" course is the definitive starting point for new SAP security professionals, providing a thorough foundation in the core security requirements of DoD Manual 5205.07.

Be prepared to dive into practical, hands-on exercises that bring the material to life, building confidence and skills to excel in your role. Choose from course dates below and register today!

Introduction to Special Access Programs (SA101.01)

- April 21 - 24, 2026 (Linthicum, Md.)
- May 12 - 15, 2026 (Linthicum, Md.)
- June 1 - 9, 2026 (Virtual)
- Aug. 4 - 7, 2026 (San Diego, Calif.)
- Aug. 25 - 28, 2026 (Cincinnati, Ohio)

Orientation to SAP Security Compliance Inspections (SA210.01)

- Aug. 31 - Sept. 1, 2026 (Cincinnati, Ohio)

SAP Mid-Level Security Management (SA201.01)

- July 13 - 17, 2026 (Linthicum, Md.)

FY 2026 UPCOMING COURSES

Registration Now Open

CDSE courses are a great way to gain security knowledge, gain awareness, and expand skill sets. Secure your spot now as classes fill quickly! **Available** courses are listed below.

Cybersecurity
Assessing Risk and Applying Security Controls to NISP Systems (CS301.01)
- May 4 - 8, 2026 (Linthicum, Md.)
- Aug. 17 - 21, 2026 (Linthicum, Md.)

General Security
DOD Security Specialist (GS101.01)
- June 2 - 10, 2026 (Linthicum, Md.)
- Aug. 11 - 19, 2026 (Germany)
- Sept. 15 - 23, 2026 (Linthicum, Md.)

DOD Security Specialist (GS101.01)
- July 6 - Aug. 2, 2026 (Virtual)

Industrial Security
Getting Started Seminar for New Facility Security Officers (IS121.10)
- May 12 - 15, 2026 (Virtual)
- July 21 - 24, 2026 (Virtual)

Information Security
Activity Security Manager (IF203.10)
- April 19 - May 17, 2026 (Virtual)
- July 26 - Aug. 23, 2026 (Virtual)

Insider Threat
Insider Threat Detection Analysis Course (INT200.10)
- April 13 - 17, 2026 (Virtual)
- May 11 - 15, 2026 (Virtual)
- June 8 - 12, 2026 (Virtual)
- July 13 - 17, 2026 (Virtual)
- Aug. 17 - 21, 2026 (Virtual)
- Sept. 21 - 25, 2026 (Virtual)

Personnel Vetting
Advanced National Security Adjudication (PS301.10)
- June 1 - 11, 2026 (Virtual)
- Sept. 14 - 24, 2026 (Virtual)

Fundamentals of National Security Adjudications (PS101.10)
- April 20 - 29, 2026 (Virtual)
- July 20 - 29, 2026 (Virtual)

Physical Security
Physical Security and Asset Protection (PY201.01)
- May 11 - 15, 2026 (Linthicum, Md.)
- June 8 - 12, 2026 (Linthicum, Md.)
- Sept. 14 - 18, 2026 (Linthicum, Md.)

STAFF SPOTLIGHT

Staff Spotlight: Stefania Fiorentino, Management and Program Analyst

By Tammi Bush

Stefania Fiorentino's work as a management and program analyst is pivotal in providing insightful analysis and data to continuously improve processes within Security Training.

As a Continuous Process Improvement (CPI) lead, Fiorentino strives to reduce costs, minimize waste, enhance engagement, and pursue innovation. She uses the define, measure, analyze, improve, control (DMAIC) method, a structured problem-solving approach to improve existing processes that don't meet performance standards or customer expectations. Under this tactic, each project phase builds on the previous one, with the goal of implementing long-term solutions to problems.

"I provide general analysis of information and data for my colleagues for quick win opportunities," Fiorentino said. "Using the DMAIC method, I hope to eliminate waste, maximize customer value, maximize efficiency, reduce risk, optimize resource allocation, and enhance operational effectiveness."

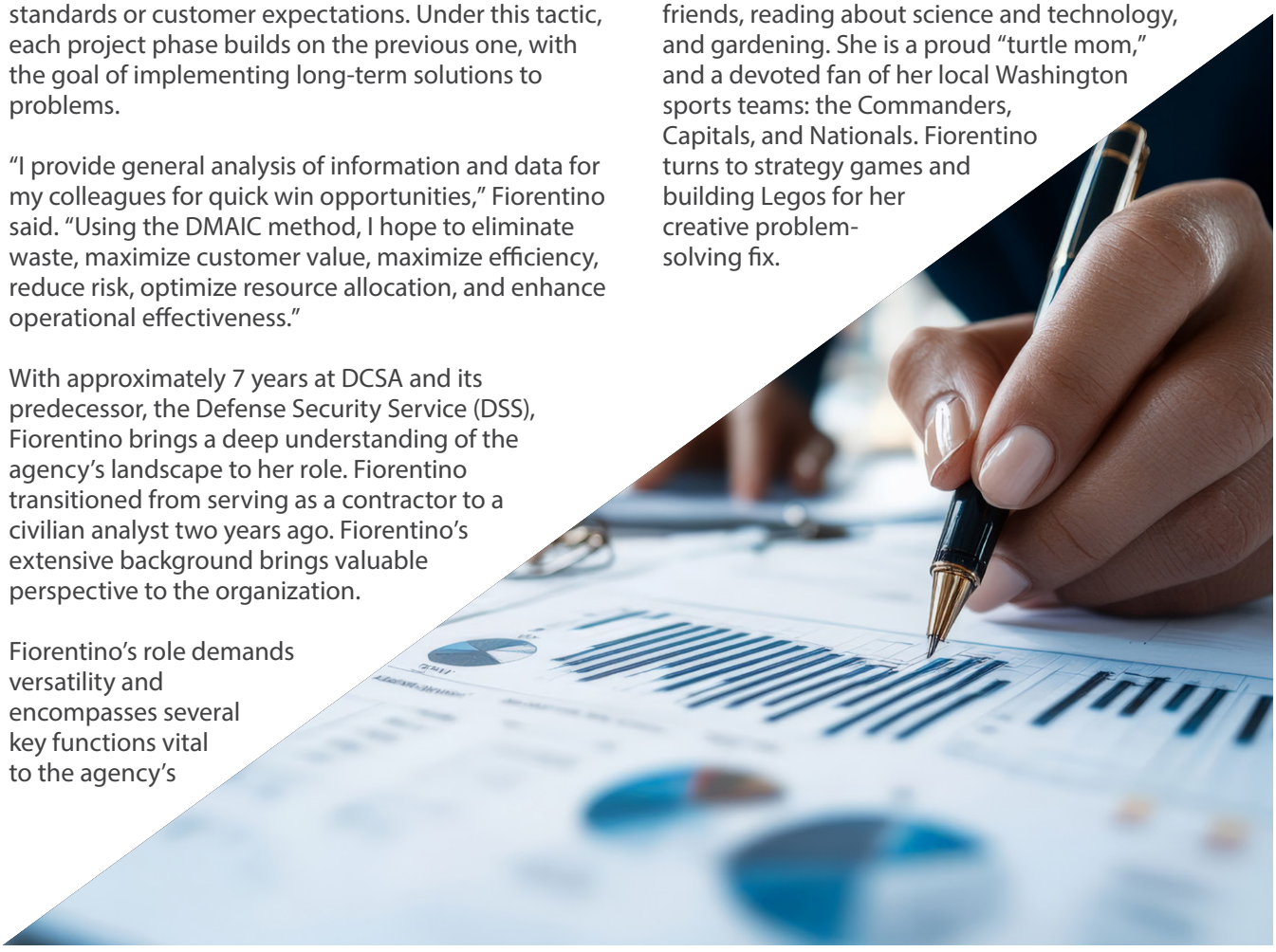
With approximately 7 years at DCSA and its predecessor, the Defense Security Service (DSS), Fiorentino brings a deep understanding of the agency's landscape to her role. Fiorentino transitioned from serving as a contractor to a civilian analyst two years ago. Fiorentino's extensive background brings valuable perspective to the organization.

Fiorentino's role demands versatility and encompasses several key functions vital to the agency's strategic goals by aligning CPI and ERM programs, which are managed by the Business Transformation Office and the Policy, Guidance, and Risk Management offices.

For Fiorentino, one of her favorite aspects of the job is "the challenge that process improvement brings, the analysis, and eliminating pain points for my colleagues."

For 2026 Fiorentino is focused on high-impact projects by providing analysis and tools to help streamline workflows.

When she's not analyzing processes or managing risks at work, Fiorentino enjoys spending time with friends, reading about science and technology, and gardening. She is a proud "turtle mom," and a devoted fan of her local Washington sports teams: the Commanders, Capitals, and Nationals. Fiorentino turns to strategy games and building Legos for her creative problem-solving fix.



ABOUT DCSA

The Defense Counterintelligence and Security Agency (DCSA) provides industrial security engagement and counterintelligence support to secure the trustworthiness of the U.S. government's workforce, contract support, technologies, services, and supply chains.

Our Role
We protect America's trusted workforce, trusted workspaces, and classified information. To do so, we have two fundamental missions: personnel security and industrial security. Supporting these two core missions are counterintelligence and insider threat and security training. For over 50 years, our agency has used each of these missions to meet the threats of our nation's adversaries.

How We Serve
DCSA is the largest investigative service provider in the federal government, supporting over 100 federal entities. We oversee 12,500 cleared facilities under the National Industrial Security Program (NISP). We rely on the following directorates to ensure the security of our nation's technologies and information.

Personnel Security
We deliver efficient and effective background investigations, continuous vetting, and adjudications. In doing so, we safeguard the integrity and trustworthiness of the federal and contractor workforce. We conduct background investigations for 95% of the federal government, including 105 departments and agencies. We also adjudicate 70% of the federal government's adjudicative determinations.

Industrial Security
At DCSA, we oversee 12,500 cleared facilities under the National Industrial Security Program (NISP). We make sure companies are protecting their facilities, personnel, and associated IT systems from attacks and vulnerabilities.

Counterintelligence and Insider Threat
Counterintelligence and insider threat supports both our personnel security and industrial security missions. Counterintelligence focuses on foreign insider threat while insider threat is focused on internal threat. In this mission center, we identify and stop attempts by our nation's adversaries to steal sensitive national security information and technologies.

Security Training
Our agency is comprised of nationally accredited training centers. These centers provide security training, education, and certifications for security professionals across the federal government and industry.

CDSE CONTACT LIST

Mailing/Postal Address
938 Elkridge Landing Road
Linthicum, Md 21090

STEPP (Learning Management System) Help Desk
Submit an online support request ticket or call the Help Desk at 202-753-0845 within the Washington, DC area or toll free at 833-200-0035 on weekdays from 8:30 a.m. to 6:00 p.m. Eastern Time.

508 Compliance and Accessibility
cdseaccessibility@mail.mil

Certification Division/SPēD Project Management Office
dcsa.spedcert@mail.mil

Education Division
dcsa.cdseeducation@mail.mil

Outreach and Engagement Office
dcsa.ncr.cdse.mbx.cdse-communications@mail.mil

Training Division
dcsa.cdsetraining@mail.mil

Webinars
dcsa.cdsewebinars@mail.mil

Webmaster
dcsa.cdseweb@mail.mil

Still not sure whom to contact?
dcsa.ncr.dcsa-cdse.mbx.cdse-front-office@mail.mil