THIS MONTH'S FOCUS

ANTITERRORISM AWARENESS

DCSA Leadership

David M. Cattler
Director, DCSA

Daniel J. Lecce
Deputy Director, DCSA

Kevin Jones
Assistant Director, Security Training

Erika Ragonese
Deputy Assistant Director, Security Training

CDSE Leadership

Glenn Stegall
Acting Director

Pulse Staff

Cashmere He
Chief Content Officer

Isaiah Burwell
Content Writer

Natalie Perkins
Content Developer/ Manager

Matthew Wright
Tammi Bush
Content Contributors

Marc Pulliam
Content Designer

15 YEARS OF PROMOTING ANTITERRORISM AWARENESS

This August marks the 15th anniversary of Antiterrorism (AT) Awareness month. The purpose of this month is to educate and remind organizations and individuals to be aware of the warning signs of terrorist activity. Individuals and organizations must also be aware of the correct procedures to follow if they recognize any of those signs.

According to the Office of the Director of National Intelligence 2024 Annual Threat Assessment, the United States faces an increasingly fragile global order strained by accelerating strategic competition among major powers. There are also more intense and unpredictable transnational challenges, and multiple regional conflicts with far-reaching implications. "An ambitious but anxious China, a confrontational Russia, some regional powers, such as Iran, and more capable non-state actors are challenging longstanding rules of the international system as well as U.S. primacy within it. Simultaneously, new technologies, fragilities in the public health sector, and environmental changes are more frequent, often have global impact, and are harder to forecast."

The Department of Homeland Security's (DHS) "See Something, Say Something" campaign and website offer a plethora of valuable antiterrorism information and how to report it. For instance, they list several warning signs of potential terrorist activity. These suspicious activities include

WHAT TYPES OF SUSPICIOUS ACTIVITIES DO I REPORT?

- Unauthorized personnel photographing, drawing, or measuring important buildings
- Unknown personnel asking questions about security forces or security procedures
- Unattended briefcase, bag, or package
- Any vehicle left in "No Parking" zones close to important buildings
- Unauthorized access to secure or sensitive areas
- Personnel wearing big, bulky clothing too hot for the weather
- Unexplained chemical smells or fumes
- Questions or requests concerning sensitive information, such as building blueprints, security plans, or VIP travel schedules without a right or need to know
- Personnel purchasing supplies or equipment that can be used to make bombs or weapons
- Unauthorized uniform puchases
- Any other situation/activity/behavior not listed that you deem as a possible safety, security, or criminal issue should be reported to security or local law enforcement

expressed or implied threats, aviation activity, testing or probing security, and numerous others. The "**See Something, Say Something" campaign website** also provides an interactive map where you can click on a state, and it will give you a number to call to report suspicious activity.

There are also multiple warning systems that advise personnel about the terrorist threat levels in their locations. Those systems are Force Protection Condition (FPCON), DOD Terrorism Threat Levels, and the National Terrorism Advisory System (NTAS).

FPCON is a DOD-approved system which standardizes DOD's identification of, and recommended preventive actions and responses to, terrorist threats against U.S. personnel and facilities. These FPCON measures change as the threat of attack changes. The lowest level is FPCON Normal and applies when a general global threat of possible terrorist activity exists and warrants a routine security posture. The highest level is FPCON Delta and applies in the immediate area where a terrorist attack has occurred or when intelligence indicates there will be imminent terrorist action against a specific location or person.

The Defense Intelligence Agency (DIA) assesses a terrorist threat level for each country. Other U.S. agencies also contribute to collecting and analyzing terrorist threat information and intelligence to ensure the best possible warning of terrorist dangers. If there is indication that a terrorist group is operationally active and targeting U.S. forces, the DIA will issue a terrorism warning report. Regional and local U.S. commanders can assign a different terrorist threat level for specific personnel, units, and installations. These threat levels inform DOD personnel of the need to take appropriate precautions.

The DHS's NTAS advisories provide timely, detailed information regarding terrorist threats to the public, Government agencies, first responders, public sector organizations, airports, and other transportation hubs. The advisories use available information to provide a concise summary of the potential threat, information about actions being taken to ensure public safety, and recommended steps that individuals, communities, businesses, and Governments can take to help prevent, mitigate, or respond to the threat.

CDSE also offers antiterrorism training and resources for individuals and organizations to share with their personnel. CDSE has the Antiterrorism Officer Level II course. This course meets the training requirements outlined in DODI O-2000.16 "Department of Defense (DOD) Antiterrorism (AT) Program Implementation" as refresher training and may be used to recertify Antiterrorism Officers (ATOs) based on component

| FPCON NORMAL	This condition applies when a general global threat of possible terrorist activity exists and warrants a routine security posture. At a minimum, access control will be conducted at all DOD installations and facilities.
FPCON ALPHA	This condition applies when there is a general threat of possible terrorist activity against personnel and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of FPCON Bravo measures. The measures in this force protection condition must be capable of being maintained indefinitely.
FPCON BRAVO	This condition applies when an increased and more predictable threat of terrorist activity exists. The measures in this FPCON must be capable of being maintained for weeks without causing undue hardship, affecting operational capability, and aggravating relations with local authorities.
FPCON CHARLIE	This condition applies when an incident occurs, or intelligence is received indicating some form of terrorist action against personnel and facilities is likely. Implementation of measures in this FPCON for more than a short period probably will create hardship and affect the peacetime activities of the unit and its personnel.
FPCON DELTA	This condition applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is imminent. Normally, this FPCON is declared as a localized condition.

DOD TERRORISM LEVELS

- **HIGH**: Anti-U.S. terrorists are operationally active and use large casualty-producing attacks as their preferred method of operation. There is a substantial DOD presence and the operating environment favors the terrorists.

- **SIGNIFICANT**: Anti-U.S. terrorists are present and attack personnel as their preferred method of operation or a group uses large casualty-producing attacks as its preferred method, but has limited operational activity. The operating environment is neutral.

- **MODERATE**: Terrorists are present, but there are no indications of anti-U.S. activity. The operating environment favors the host nation and the U.S.

- **LOW**: No terrorist group is detected or the group activity is non-threatening.

approvals. It details the duties and responsibilities of ATOs at DOD facilities or installations around the world; discusses AT awareness; terrorist group operations; hostage-taking and survival; terrorist use of weapons of mass destruction; active shooter threat and insider threat; and explores the AT plan by examining physical security considerations, the antiterrorism planning process, and resource management. CDSE's antiterrorism resources include other eLearning courses, security awareness games, job aids, toolkits, and shorts.

The resources offered by DOD, DHS, DIA, CDSE, and the State Department are tools to refresh your antiterrorism knowledge. Organizations should continuously train and prepare their employees about terrorist warning signs, force protection practices, and reporting suspicious activities and threats. Individuals should remain vigilant against terrorist threats and make the effort to learn how to avoid potential threats, protect themselves, and report when needed. Protecting the Nation, your organization, and yourself against terrorist threats is a year-round team effort.
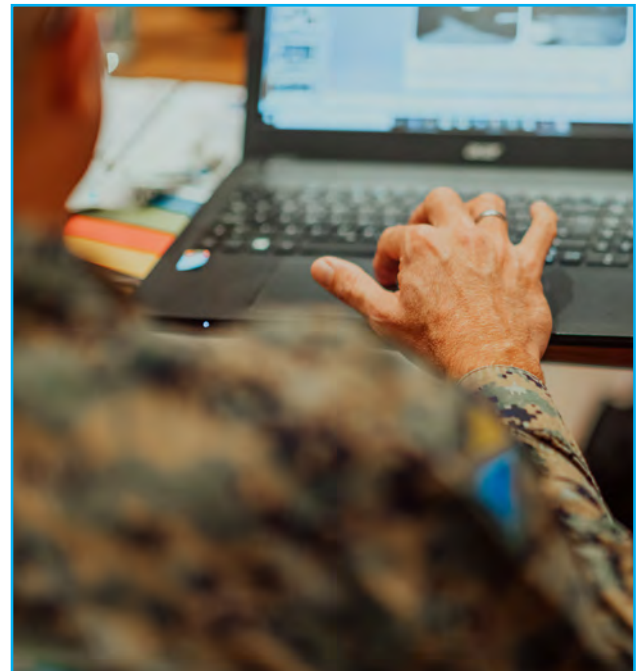
CDSE AND DOD ANTITERRORISM RESOURCES

PRODUCT	TYPE
Antiterrorism Officer Level II (GS109.16)	eLearning Course
Antiterrorism Considerations and Design/Construction Standards	Physical Security Toolkit (Physical Security Planning Tab)
Active Shooter Awareness	Short
CI Foreign Travel Brief	Short
DOD CI Awareness and Reporting Course for DOD Employees (CI116.16)	eLearning Course
Targeted Violence Security Awareness	Security Awareness Game
CJCS Guide 5260, A Self Help Guide to Antiterrorism	Job Aid/Guide
Antiterrorism Individual Protective Measures Card	Job Aid/Pocket Card
Insider Threat Toolkit (Kinetic Violence Tab)	Job Aids/ Reports/ Videos / Policy/ Training
Insider Threat and Extremist Activity Within the DOD	Job Aid/ Briefing

OTHER FEDERAL AGENCY ANTITERRORISM RESOURCES

PRODUCT	SOURCE
Traveler Resources	U.S. Department of State
Counterterrorism Guide	Office of the Director for National Intelligence
Joint Communication Assessment Team (JCAT) Products and Resources	Office of the Director for National Intelligence
Preventing Terrorism	Department of Homeland Security
See Something/Say Something	Department of Homeland Security
National Terrorism Advisory Alerts/Bulletins	Department of Homeland Security

2024 DCSA SECURITY CONFERENCE FOR DOD

The 2024 DCSA Security Conference for DOD was held on August 6-8! This year's conference theme was "Collaboration: Breaking Down Barriers." The agenda included topics such as insider threat, controlled unclassified information, personnel security vetting, policy updates, and more. If you missed the conference or would like to revisit the different sessions' content, the presentations/recordings will be made available online to registered participants.

INSTRUCTOR-LED CYBERSECURITY COURSE AT CDSE IN DECEMBER

CDSE is offering an instructor-led training (ILT) course on Assessing Risk and Applying Security Controls to NISP Systems (CS301.01) in December This course is tuition free and runs December 2-5 in Linthicum, MD. Students should have completed enrollment (prerequisites and registration) by November 14.

The target audience for this training includes Information System Security Managers (ISSMs), Information System Security Officers, and FSOs involved in the planning, management, and execution of security programs for cleared industry. This course provides students with guidance on applying policies and standards used throughout the U.S. Government to protect information within computer systems, as delineated by the risk management framework process.

Go **here** to learn more, register, and view the required prerequisites.

PERSONNEL VETTING SEMINAR

CDSE is presenting the virtual instructor-led (VILT) Personnel Vetting Seminar on December 9-19. This seminar addresses the requirements associated with the reform of the Federal Government's personnel vetting system, which is known as Trusted Workforce (TW) 2.0. Its purpose is to aid personnel vetting practitioners in DOD, federal agencies, and private industry understand TW 2.0 requirements, identify gaps between current and future procedures, and provide support through the implementation process. The seminar covers topics such as end-to-end personnel vetting operations, including the federal background investigations program, National Security Adjudications, Continuous Vetting, and Insider Threat analysis in a collaborative environment.

This course is intended for U.S. Government security professionals, military personnel, cleared industry Facility Security Officers (FSOs), and other federal personnel performing personnel vetting security-related duties, as well as personnel executing security programs for cleared industry. Visit the **course page** to learn more and register.

2024 DCSA CONFERENCE FOR INSIDER THREAT (NITAM) REGISTRATION NOW AVAILABLE

Registration is open for the DCSA Conference for Insider Threat in support of National Insider Threat Awareness Month (NITAM). The conference theme is "Deter, Detect, Mitigate" and will be held in-person and virtually on September 9-10, 2024. Registration for in-person attendance for this event will close August 26. Visit the registration website to learn more about the event and **register**.

The NITAM website is also available for viewing **here**.

UPCOMING WEBINARS

CDSE webinars are a great way to gain insight into various security topics and interact with security experts. Webinars can also be used as professional development units (PDUs) in support of SPēD certification maintenance. Sign up today for the following upcoming live webinars:

Security Rating Score Tool and Resources
August 29, 2024
1:00 p.m. to 2:30 p.m. ET

Mass Shooter Contagion Theory and the Copycat Effect in the Evolving Media Environment
September 5, 2024
12:00 p.m. to 1:30 p.m. ET

Security Professional Trusted Workforce 2.0
September 17, 2024
1:00 p.m. to 2:30 p.m. ET

Click **here** to register for these events and join the discussion!

NINTH ANNUAL COUNTER-INSIDER THREAT (C-InT) SYMPOSIUM

National Insider Threat Awareness Month (NITAM) kicks off this year with the Ninth Annual C-InT Symposium, taking place September 4-5 in Washington, D.C. DCSA is pleased to participate in this event that promises to bring together leading experts from Government, industry, and academia to share insights and strategies to combat insider risks.

Don't miss this opportunity to network, learn from distinguished speakers, and discover the latest advancements in insider threat detection and mitigation. Register now at **counterinsider.com** to be part of this important discussion.

Active-duty U.S. military and Government personnel attend free. Please email Joe Trupia at **jtrupia@ dsigroup.org** for details.

FY 2024/25 UPCOMING COURSES

The FY25 course schedule has been released. Consider signing up for one of CDSE's remaining FY24 or upcoming ILT or VILT courses. Training is free and travel expenses are eliminated for VILT courses. CDSE courses earn PDUs toward maintenance of SPēD Program certifications and credentials. Select courses also have ACE CREDIT recommendations that may earn transfer credits at participating universities and/or are approved for CEU credit toward some CompTIA certification renewals. Access the **training schedule** today to learn more and secure your spot. Below is a list of ILT/VILT courses available in September and November. All ILT iterations are located at Linthicum, MD, unless indicated otherwise.

COURSE	DATE	RECOMMENDATION
DOD Security Specialist	**Sept. 17 - 25** (ILT) **Oct. 22 - 31** (ILT) **Nov. 18 - Dec. 15** (VILT)	ACE CREDIT CompTIA
Getting Started Seminar for New Facility Security Officers	**Oct. 22 - 25** (VILT)	
Activity Security Manager	**Oct. 20 - Nov. 17** (VILT)	ACE CREDIT CompTIA
Physical Security and Asset Protection	**Oct. 21 - 25** (ILT) **Nov. 4 - 22** (VILT)	CompTIA
Insider Threat Detection Analysis Course (ITDAC)	**Oct . 7 - 11** (VILT) **Nov. 18 - 22** (VILT)	
SAP Mid-Level Security Management	**Nov. 18 - 22** (ILT)	ACE CREDIT CompTIA
Personnel Vetting Management Seminar	**Nov. 19 - 21** (VILT)	
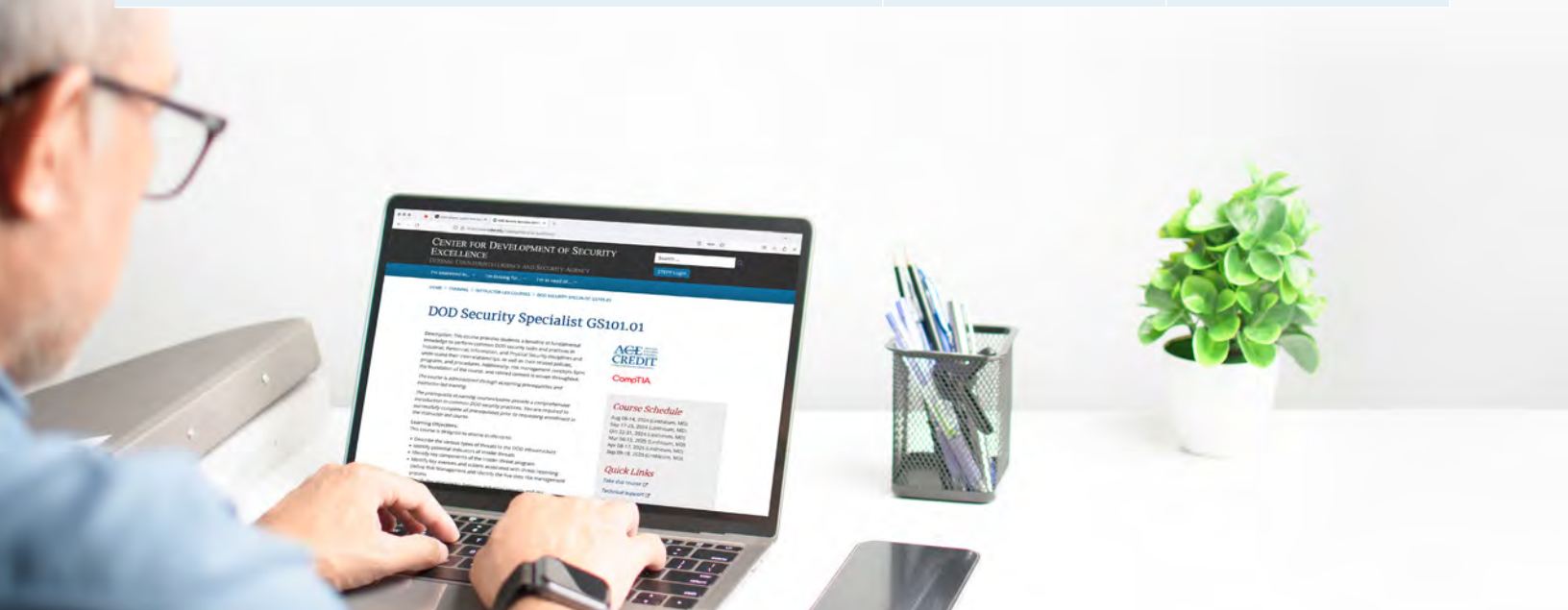
★★★★★ **WHAT THE SECURITY COMMUNITY IS SAYING ABOUT THE 2024 DCSA SECURITY CONFERENCE FOR DOD**

"Good information about where the Security community is today and what is coming in the future."

"A lot of great information was provided and I really do appreciate all the SMEs giving us all the updated information and a way ahead on what we are to expect."

"I like the updates on policy and where they are in the process, particularly the DoDM 5105.21."

"Behavioral Health piece was great."

"Very informative. I am glad that we are getting updates of the policies and regulations."

"Awesome...integration and policy updates are key to our success."

"Change is coming in all aspects of security and to stay aware of the policy and operational changes."

"Really enjoyed the discussion from Dr. Priester on psych."

"I liked the DCSA briefs."

"All of the information was very helpful."

CDSE NEWS

CDSE offers an email subscriber news service to get the latest CDSE news, updates, and information. You may be receiving the Pulse through your subscription, but if you were forwarded this newsletter from another source and would like to subscribe to the Pulse or one of our other topics, visit our **news page** and sign up or update your account today.