2024

AIRE

Advancement of Insider Risk Education

JOURNAL

CDSE Center for Development of Security Excellence

LEARN. PERFORM. PROTECT.

Advancement of Insider Risk Education Journal

An annual publication for the professionalization of counter-insider threat program personnel.

For the first issue of *AIRE*, readers will find a collection of training, education, and professionalization efforts related to mitigating insider risk. This publication aims to offer an in-depth look at available resources, training needs, development, trends, and challenges across the DOD, USG, and industry. The need to expand a resilient workforce that is prepared to recognize and respond to insiders that may use their authorized access to cause harm has not waned. We hope the security community, specifically, those individuals charged with providing insider risk training, education, and professionalization options to their workforce, find this to be a useful tool. Share with colleagues and senior leaders, and participate in a unified effort to expand a shared network of knowledge and capabilities for all.

IN THIS ISSUE

Three priorities – defending the nation, taking care of our people, and succeeding through team work – will guide our efforts.

– Secretary of Defense
Lloyd J. Austin III
March 4, 2021

WHAT THE CDSE CAN OFFER YOU

CDSE provides a wide variety of products and services to address security education, training, awareness, and professionalization needs. We deliver our products across the industrial, information, personnel, and physical security disciplines as well as other functional areas such as Special Access Programs. Over the years, numerous agencies and organizations have relied on CDSE's education and training programs to assist in strengthening their own security programs.

CDSE Education Program offers certificates in five concentrations. Students can earn certifications in Risk Management, Security Leadership, Security Management, Security (Generalist), and Systems Operations. Students are recognized for successfully completing an advanced program of study. CDSE Education certifications are ideal for individuals who are interested in adding to their credentials as Security Professionals.

CDSE Training Program provides a multitude of courses and products to include Collegiate-level Education Courses, Instructor-led Training, eLearning, Webinars, Security Shorts, Performance Support Tools, and SPēD Certification Program. CDSE offers courses and products to employees of federal agencies, DOD contractors, DOD personnel, as well as selected foreign governments. CDSE courses are offered through various platform insuring specified requirements are met.

SPēD Certification Program: The Security Professional Education Development (SPēD) Certification Program is part of the Department of Defense's (DOD) initiative to professionalize the security workforce. The SPēD Certification Program ensures there is a common set of competencies among security practitioners. This initiative promotes interoperability, facilitates professional development and training, and develops a workforce of certified security professionals.

Insider Threat is the potential for an insider to use their authorized access or understanding of an organization to intentionally or unintentionally harm that organization. CDSE's Insider Threat Programs deter, detect, and mitigate actions by insiders that pose a threat to national security. CDSE offers a wide variety of products that assists individuals in developing a foundation in the Insider Threat Program, as well as its principles and concepts.

Counterintelligence protects an agency's intelligence program from an opposition's intelligence service. CDSE's counterintelligence (CI) Awareness Program helps to identify various threats from illicit collectors of U.S. defense information, foreign intelligence entities, and terrorist. The Counterintelligence (CI) Awareness Program makes DOD and Industry Security personnel aware of their responsibility to report suspicious behaviors or activities.

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. CDSE offers a variety of training products to assist one in developing a foundation in Cybersecurity concepts and principles.

Physical security is security measures that deny unauthorized access to facilities, equipment, and protect personnel and property from damage or harm. The Physical Security (PHYSEC) Program is comprised of active and passive measure, intended to prevent the unauthorized access to personnel, equipment, installations, materials, and information. CDSE offers a variety of training products to assist one in developing a foundation in PHYSEC concepts and principles.

Personnel security (PS) establishes the standards, criteria, and guidelines upon which personnel security eligibility determinations are based. CDSE offers a variety of training products to assist one in expanding their PS knowledge and skills.

General Security covers security topics and issues that could be addressed in other security disciplines and content areas. CDSE offers a variety of training products to assist one in expanding their General Security knowledge and skills.

Industrial Security is a portion of internal security that refers to the protection of industrial installations, resources, and classified information essential to protect from loss or damage. The Industrial Security Program is a multi-disciplinary security program that focuses on the protection of classified information developed by, or entrusted to, U.S. industry operating under the National Industrial Security Program (NISP). CDSE offers a variety or training products to assist one in expanding their Industrial Security knowledge and skills.

Information Security is procedures or measures used to protect electronic data from unauthorized access or use. The Information Security (INFOSEC) Program establishes policies, procedures, and requirements to protect classified and controlled unclassified information (CUI) that, if disclosed, could cause damage to national security. CDSE offers a variety or training products to assist one in expanding their INFOSEC knowledge and skills.

Operations Security (OPSEC) is the process by which we protect critical information, both classified and unclassified, that can be used against us. It focuses on preventing our adversaries' access to information and actions that may compromise an operation. OPSEC challenges us to look at ourselves through the eyes of an adversary and deny the adversary the ability to act. CDSE offers self-paced eLearning courses that expand one's knowledge and skills in this area.

Special Access Program is for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level. CDSE offers a variety of training products to assist one in expanding their knowledge and skills in this area. ■

You can learn more about these training and education programs by visiting the Center for Development of Security Excellence website.

The CDSE Pulse newsletter gives a monthly snapshot that focuses on one area of interest and the CDSE products associated with it. Subscribe for CDSE news and updates.

HIGHLIGHTED **TRAINING PRODUCTS**

ELEARNING INT101: INSIDER THREAT AWARENESS

In 2012, President Barack Obama signed a memorandum for the National Insider Threat Policy Minimum Standards for Executive Insider Threat Programs. Enclosed within this memorandum are specific elements required to establish effective insider threat programs, develop their capabilities to strengthen protection of classified information, and bolster defense against adversaries and insiders who utilize their access intentionally or unintentionally to harm national security.

By Amber Jackson
Intelligence Operations Specialist, Insider Threat
Center for Development of Security Excellence

These minimum standards state the requirement of government agencies to provide their employees with insider threat training and awareness. This training may be in-person or virtual and should be provided to employees with both national security eligibility and access to classified information.

Awareness training should at a minimum cover:

- The importance of detecting potential insider threats by employees with national security eligibility
- The importance of reporting concerning behavior to insider threat personnel and other designated officials
- Approaches and means used by adversaries to recruit insiders and collect classified information
- Indicators of potential insider threat behaviors and procedures to report those behaviors
- Counterintelligence and security reporting requirements

In order to help meet this requirement, CDSE released eLearning course CI121.06: Insider Threat Awareness in 2013. This course provided a thorough understanding of how insider threat awareness is an essential component of any comprehensive security program. It endorsed the national campaign slogan, "If you see something, say something," adopted by the Department of Homeland Security from the New York Metropolitan Transit Authority after the terrorist attack on September 11, 2011, to help emphasize the importance of reporting suspicious activity.

As a foundational course, CI121 received various updates to improve its explanation of adversarial and recruitment methodology and real-world examples and to better explain content covered in lessons such as the Scope of the Insider Threats and Their Targets, Insider Threat Indicators, and Reporting a Potential Threat before receiving a complete refresh in 2017 as INT101.16.

Multiple policies and memorandums were included as references during the developmental stage of the newer course. This included but was not limited to the following:

- Department of Defense Directive 5205.16: The DOD Insider Threat Program; September 30, 2014
- 32 CFR Part 117 NISPOM Rule (formerly DOD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), Change 2; May 18, 2016)
- Department of Defense Manual 5200.01, Volumes 1-3: DOD Information Security Program; February 24, 2012
- DITMAC Memorandum
- PAR Memorandum
- Unauthorized Disclosure Memorandum

The course underwent a visual redesign and received another update of case study materials to cover lessons on Insider Threat, Potential Indicators of an Insider Threat, and Reporting. With an estimated completion time of 30 minutes, the course was satisfactory and successful for its target audience of DOD civilian employees and defense contractors, personnel with and without national security eligibility.

STUDENT FEEDBACK, 2017-2018

2017:

"This was actually a good one. It was short and to the point. So good job."

"This is a good example of a course that is an annual requirement. Very focused on just the knowledge required without going into too much detail. The information was very helpful and was a great refresher."

2018:

"This training was excellent. I gave briefs on insider threats in the military and this training was one of the best I have seen. Great job on covering the topics, making it relatable, and explaining the dangers."

"This course was easy to follow, flowed well and made sense. More trainings should follow this structure."

"We just received a coworker who tried to do something similar to this. By using these skills, I was able to report the new coworker to our supervisor."

Five years later, after its initial configuration, Insider Threat Awareness would enter a maintenance cycle to address stakeholder requests and student feedback and implement recommendations from a training needs analysis conducted in 2016. The 2019 maintenance cycle aimed to broaden its audience from DOD to the general federal workforce, industry, and critical infrastructure sectors while functioning as a refresher course for annual mandatory training for the federal workforce and industry. This version of INT101 would utilize case study scenarios, teach the common indicators that highlight actions and behaviors that can signify an insider threat, and promote a proactive approach to reporting suspicious activities. Upon completion, students would be able to recognize suspicious behavior and activity associated with the insider threat and identify reporting requirements in 60 minutes.

Subsequently, there was a desire from students and stakeholders alike to streamline annual mandatory training. Other eLearnings had successfully incorporated test-out opportunities within their course frameworks, reducing the time spent completing refresher training. In 2020, INT101 would get a similar treatment. A modified version that included a test-out activity deployed in fall of 2021.

This effort brought in mixed reviews. Facility security officers that utilized INT101 and students who enrolled into the course fell on either extreme of the perceived efficacy of the test-out option. While some enjoyed the abbreviated alternative, which allowed them to skip unrefreshed or repetitive materials, others believed it was too simplistic, lacked prompts for critical thought, and circumvented awareness training requirements rather than refresh them.

STUDENT FEEDBACK, 2021-2022

2021:

"I've been doing this for over 50 years; it's always good to get the refresher! However, to be more realistic I think you should tone down your aggressive reading of the situations you present. Sometimes a request to submit a paper to a journal or at a conference is just a request to make a presentation -- it is generally NOT an actionable offense!

2022:

"This is one of the best Training Course I've taken in my 30 years in industry. Clear, straight to the point, now sneaky questions; just clear real world situations we all are exposed to as scenarios, with straightforward answers. Audio was excellent too. Pages loaded fast too. Wish all training was this good!"

"All reoccurring training courses should be broken down like this. If we've taken the basic course and retained the material we should not have to complete all that again. So this was very informative, jogged my memory about insider threat, and didn't use up a lot of my time."

"Again, the previous insider threat training offered was much better. I do NOT work in a SCIF environment, so a lot of this doesn't necessarily apply to me, but with this training it is VERY obvious that the only good answer is to 'report everything.' I am not sure this is necessarily the best work environment for anyone, and it also allows the average worker to abdicate critical thinking about the problem and encourages mindless paranoia."

With such a controversial split over the test-out option, it was clear its inclusion needed a revaluation, and perhaps even removal. In 2022, CDSE decided additional maintenance was not the best course of action but rather a new course could be delivered to address the concerns of students and stakeholders. A new course might offer a new insider threat awareness experience where students would be required to use critical thinking for activities in scenario-based training modules—an experience where one must decide more than if they should report concerning behavior, but also the application of what and to whom/where they should report. This new course might underscore salient topics, such as unauthorized disclosures and legitimate whistleblower activities protections, and place proper context around behaviors associated with domestic violent extremism, ultimately inspired by the Secretary of Defense's mandated stand-down to address extremism in ranks in 2021.

The test-out option may be on its way out; however, CDSE is committed to deploying security training, education, and awareness resources that tie policy with innovation. This includes keeping materials timely, accurate, and effective for its audience. The current version of INT101 meets national and DOD policy requirements. A new version of INT101 Insider Threat Awareness is estimated to deploy in spring of 2024. ■

DCSA COUNTER-INSIDER THREAT COMMUNITY TRAINING SERIES

In 2022, the Analysis and Mitigation Branch of the DOD Insider Threat Management and Analysis Center (DITMAC) led a series of presentations called the "Counter-Insider Threat Community-Wide Trainings." The audience for these trainings were mainly comprised of DOD-component Insider Threat program personnel. The monthly presentations were hosted over a virtual platform for around 90 minutes and explored trending topics in DOD Insider Threat hubs. Live, unclassified discussions included domestic violence, suicide prevention, introduction to threat assessment and management, and cognitive biases.

In January of 2023, a few members of a burgeoning Behavioral Threat and Analysis Center (BTAC) reached out to CDSE to learn how to improve DITMAC's training presentations. The BTAC had assumed responsibility over the trainings and wanted to improve outreach efforts. CDSE, known for its collaborative spirit and successful security conferences, had the infrastructure, capability, and experience to produce security training webinars. Naturally, a new partnership was in the works.

In March, DITMAC and CDSE's new joint venture would come to fruition with the solid launch of the first of six training webinars. Today, the Counter Insider Threat Community Wide Trainings, now rebranded as the DCSA Counter Insider Threat Community Training Series, aims to target a larger audience across the USG, DOD, and Industry. Typically hosted on Thursday afternoons, insider threat/risk practitioners from all programs are encouraged to attend the monthly training series.

Security officers, analysts, managers, and various other security professionals have found value in attendance. Attendees can expect a 60-minute presentation from guest speakers and subject matter experts vetted by DCSA's gatekeepers, followed by a 30-minute question and answer segment. Attendees may also gain professional development units and have the opportunity to download certain presentations and related materials as training aids.

Topics covered so far in 2023 include Structured Professional Judgment Tools and Insider Threat, Radicalization to Terrorism: Psychological Processes and Research Updates, Command Directed Behavior Health vs. Fit for Duty vs. Security-Focused Medical Evaluations, and Domestic Violent Extremism.

Other topics include "Social Engineering: The Manipulated Insider," "Online Behavior in Threat Assessment," and "Insider Risk and Security Clearance Adjudications." ■

To register for future training webinars, visit the webinar page on the CDSE website.

Follow CDSE on Facebook, X (Twitter), YouTube, and LinkedIn and subscribe to Insider Threat Gov Delivery to be the first to know about upcoming training opportunities.

ATTENDEE FEEDBACK

"Way more interesting than I anticipated! "

"Great information and appreciate the examples!"

"This was an informative presentation. The length of time and use of time was perfect."

"Working with the Insider Threat Working Group[,] this will be a useful tool."

"Very informative class. I now have other tools to use when teaching/discussing insider threats in the workplace."

"The class was very useful."

INSIDER THREAT DETECTION ANALYSIS COURSE

Your boss just assigned you to your organization's insider threat hub team. So, now what? What is an insider threat hub and what are your responsibilities? ITDAC can help answer those questions.

The Insider Threat Detection Analysis Course (ITDAC) provides entry level DOD Counter-Insider Threat Analysts the ability to apply critical thinking skills and structured analytic techniques to address potential insider threat indicators. ITDAC reinforces and expands on Insider Threat fundamentals. The course teaches Insider Threat Analysts how to apply Executive Order and DOD authorities to gather data, aggregate information, analyze what it means, and how to respond to any threat identified while still ensuring that constitutional and privacy rights are protected. ITDAC goes beyond simply instruction. The course uses extensive real-world practical exercises that allow students to work together to collect information, discover gaps in what they know, request additional data, and interpret the "big picture."

ITDAC is a five-day course offered virtually through the Security Training Education and Professionalization Portal (STEPP), so you do not need to travel. Students work together from wherever they are to complete five practical exercises that include topics such as the misuse of information technology, potential workplace violence, espionage, mental health issues, and responding to continuous evaluation notifications.

ITDAC satisfies the training requirements for personnel assigned to insider threat programs identified in the Presidential Memorandum of November 21, 2012, National Insider Threat Policy and Minimum Standards of Executive Branch. These requirements are:

- Counterintelligence and security fundamentals to include applicable legal issues
- Agency procedures for conducting insider threat response action(s)
- Applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information
- Applicable civil liberties and privacy laws, regulations, and policies
- Investigative referral requirements of Section 811 of the Intelligence Authorization Act

During development, stakeholders in the DOD counter-insider threat enterprise added two additional training topics:

- Application of behavioral pathways
- An overview of the DOD counter-insider threat enterprise

Stakeholders also requested that students complete the course with an intermediate level of competency. To meet this requirement, ITDAC includes multiple practical exercises.

These initial requirements ultimately became the current learning objectives for ITDAC. After completing the course, students will be able to:

- Understand Insider Threat Hub operational and process dynamics
- Understand the processes for Hub functions to effectively gather information
- Understand the legal considerations in establishing program processes, to include handling information from a variety of internal and external sources
- Demonstrate how to gather and document counterintelligence, security, information assurance, human resource, law enforcement, and other relevant information related to potential Insider Threat activities
- Demonstrate how to integrate and analyze information on potential Insider Threat activities and recommend mitigation actions

The course was originally delivered in person at the Defense Intelligence Agency's Academy for Defense Intelligence in Washington, DC. Pilot offerings of ITDAC occurred in FY 2019 and the beginning of FY 2020. In its first year, there were only six ITDAC classes. COVID-19 brought a shift to virtual instructor-led course offerings. This shift allowed an increase in the number of offerings to eleven times a year.

The course was initially only for personnel assigned to DOD counter-insider threat programs. Supporting stakeholders such as counterintelligence, law enforcement, and security attended as space allowed. When the National Insider Threat Task Force's Insider Threat Hub Operations Course was suspended, the ITDAC started prioritizing all U.S. Government counter-insider threat personnel to attend the course.

Students attending ITDAC have included representatives of the Air Force, Army, Marine Corps, Navy, and the Coast Guard. A large number of federal agencies have also participated in the ITDAC, including the Department of Transportation (DOT), Department of Homeland Security (DHS), Transportation Security Agency (TSA), and Internal Revenue Service (IRS).

STUDENT FEEDBACK

"Exceptional instructors! They both were very knowledgeable of the content and demonstrated this by providing depth on the subject matter on every topic and focus discussion."

"I enjoyed the course and could really see how passionate Don and Julie were about the subject matter and making it interesting and engaging for students."

"The instructors did a great job making virtual learning responsive and interactive to reaffirm concepts."

"Outstanding class! Facilitators were great and the content was appropriate for the subject of the course. Kudos to the staff!"

"This was a great course and covered a breadth of Insider Threat analytic topics!"

To register for this course, visit the ITDAC page on the CDSE website.

If you any questions about the course, email the CDSE Insider Threat training team.

TOP FIVE TRENDS
FOR TRAINING DEVELOPMENT

To understand the current state of learning and development in America's workplaces, the Society for Human Resource Management (SHRM) and Talent LMS surveyed U.S.-based HR managers and employees in early 2022. The goal was to learn what employees want and expect from learning and development departments as well as what organizations are willing and able to provide.

By Stephen Ransdell
Senior Instructional Systems Designer
CDSE Insider Threat Team

The study revealed some of the major challenges in 2022. Changes in workplace dynamics, especially the shift to more remote work situations, along with a continuing evolution in learner expectations, created several new challenges to learning designers.

DECREASING LEARNER ATTENTION SPAN

Cell phones and other technologies have led to many changes in learner expectations. In the past, training took the form of in-person, long-form, classroom-based instruction. This was soon largely replaced by computer-based training. This evolution produced shorter training that could be delivered nearly anywhere at any time. Today, learner attention span has decreased greatly. Modern learners are used to accessing information immediately. Current trends in Learning and Development are attempting to address these needs. Many training managers feel overwhelmed and under equipped to produce high quality training content quickly and on a large scale.

CONTINUING FOCUS ON TRAINING COST

For large organizations, the largest learning cost isn't the cost of developing and deploying a training solution. Rather, it's the time employees spend away from their day-to-day work while taking training. This time needs to be well spent. Some typical student complaints about current training includes a resistance to reading on-screen text. Long, text-heavy, and unengaging online learning falls flat. Online learning that lacks engagement isn't working. It feels forced upon the employees and there's resistance, as they don't see the benefits or any real world application.

WHAT LEARNERS WANT

According to the SHRM survey, 43 percent of learners say they want more video content. 50 percent of learners want more personalization. Learners are demanding more people-centered learning content. The most common (and preferred) device to take training on is a laptop. While a slight majority of employees take training at a desktop computer, most would prefer to use a laptop or other device. Mobile learning is rapidly becoming the preferred deliver method. More learners are turning to tablets or phones for training. They expect training to be quick, easy, and interactive.

WHAT LEARNERS ACTUALLY GET

According to the study, 60 percent of all training courses are 30 minutes long or longer. While time allotted for training is shrinking, a majority of the training is long, text-heavy, unengaging presentations. The required time to complete training does not correspond to the time the learner has away from other job duties. There is too much focus on passing a test as opposed to learning material applicable to daily duties.

TRENDS IN TRAINING DEVELOPMENT

1. Micro Learning That Is Truly Micro
Training managers across industry have stated that addressing the shortened attention span of learners is a paramount concern. This is reflected in growing trend towards micro learning that really is micro. Within the industry there is a definite, and growing, move to shorter learning experiences. The current average for this type of training is now 8 minutes or less. More training managers are moving away from structured courses and towards providing learning resources. These learning resources can then be packaged into self-guided learning programs.

2. More Video-Based Learning
41 percent of learning and development leaders are looking to push video learning in the coming year. To meet learner demand, new content development is incorporating more user generated stories. These stories leverage peer-to-peer learning as a fast-growing trend. This content is then packaged in self-directed training programs.

3. Flexible Blended Learning
The recent pandemic and the associated stay-at-home mandates forced training managers to pivot and develop ways to deliver training content solely through remote means. As the situation continued, many employers discovered the value in fostering this new trend. In many organizations, employees are not anxious to return to old working paradigms. They prefer a blended approach that uses many different training modalities instead. Learners are looking for more personalized and inclusive learning that is available as needed, where needed. Training managers are packaging these learning components into programs that produce numerous self-paced learning triumphs incorporating alternative recognitions of success, such as badging.

4. Accessibility Is the New Theme
Within the learning and development field, there are several trends that could make training more self-directed and modular. These include:

- **Learning in the Moment of Need (just-in-time training):** Training and performance support tools that can be leveraged to support immediate training when needed, anytime, anywhere.
- **Content Repurposing:** The push toward micro learning allows content to be reused where needed without requiring that it be reproduced. These micro learnings can be packaged together in numerous ways to create more personalized, self-directed learning programs.

5. Other Growing Training Trends:

- **Virtual Reality (VR)/Simulation:** Some learners desire more VR and simulation in training products. Learners appreciate a chance to perform a task virtually without the real-world consequences of missteps. However, these training approaches are still costly and time consuming to produce. Many training managers stated that they are looking to use Artificial Intelligence in their future training products.
- **Podcasting:** There is a growing trend within the training industry to employ podcasting to augment other training efforts. Podcasts allow an organization to deliver training content that may leverage peer-to-peer training. It also allows a fast response to a general training need as either a stop-gap solution until a more permanent solution can be developed, or as just-in-time training. ■

ABOUT THE AUTHOR

Stephen Ransdell serves as the Senior Instructional Systems Designer for the Center for Defense Security Excellence Insider Threat Team. He has worked with a wide variety of government and private Industry clients including the Department of Defense, Federal Aviation Administration, and the Department of Veterans Affairs. Mr. Ransdell has over 30 years of experience in training analysis, development, and delivery and evaluation.

The Center for Development of Security Excellence offers a wide variety of dynamic learning products that range from interactive online games to training videos. To learn more, visit the CDSE website and YouTube channel.

HIGHLIGHTED **EDUCATION PRODUCTS**

ED 520: FOUNDATIONS OF INSIDER THREAT MANAGEMENT

Interested in learning how to manage insider threats? Read our Q&A to see if ED520 might be for you.

WHAT IS ED 520: FOUNDATIONS OF INSIDER THREAT?

The Center for Development of Security Excellence (CDSE), Defense Counterintelligence and Security Agency (DCSA) offers 18 education courses (ED) to U.S. military members and civilian government employees. Among those courses is ED 520: Foundations of Insider Threat Management, a 16-week-long, graduate-level course designed to introduce students to the risks posed by trusted insiders, including the psychological motivations, predispositions, and behaviors associated with this group. The course delivery method is virtual instructor-led education (VILE) via the Security, Education, Training and Professionalization Portal (STEPP), and each course iteration has a 20-student capacity and five-student waitlist.

WHAT ARE THE STUDENT DEMOGRAPHICS?

The student makeup is very diverse, ranging from full-time insider threat practitioners with years of experience to those new or not yet exposed to insider threat programs. There have been students from near and far, to include Japan, with a 13- to 14-hour time zone difference, as well as students from various U.S. locations. Since the course is virtual, students can complete their assignments at their convenience.

DOES THE INSTRUCTOR EVER ENGAGE LIVE WITH THE STUDENTS?

The instructor conducts periodic telephone conferences with the students to engage with them, which helps foster effective rapport and connection with them. He also engages with them via STEPP and email.

WHAT IS THE BACKGROUND OF THE COURSE?

ED 520 started in late 2019 when CDSE collaborated with the Office of the Under Secretary of Defense for Intelligence and Security (OUSD (I&S)) and the National Insider Threat Task Force (NITTF). With these partners, CDSE developed the first pilot graduate-level insider threat course for academia. In 2020, it received the approval to pilot the course at Marymount University. CDSE then applied the best practices and framework to develop a course for the DOD. In January 2021, CDSE offered the first iteration of ED 520, Foundations of Insider Threat Management.

WHAT IS THE OVERALL OBJECTIVE OF THE COURSE?

Students explore the historical context of insider threat and the counter-insider threat mission, to include relevant law, policy, and regulation. Students are challenged to apply critical thinking skills to address current issues surrounding this problem set, including privacy and civil liberties concerns, cyber insider threat, and active shooter/workplace violence. Students contextualize these issues within their major area of study to identify the role of their discipline in preventing and countering insider threats.

WHAT ARE THE OTHER COURSE OBJECTIVES?

The course will enable students to assess risks posed by trusted insiders and specific psychological factors that contribute to risk; evaluate the historical context for insider threat and the impact of political and socioeconomic factors on threat behavior and incident response; critique current policies and programs designed to counter the insider threat and relate multi-disciplinary risk mitigation actions to their field of study; differentiate Government and private sector insider threat response; evaluate specific problem sets related to privacy and civil liberties concerns, cyber insider threat, and acts of violence; and appraise the current state of social and behavioral science research into insider threat and propose future areas of research to address insider threats.

WHAT ARE THE COURSE COMMITMENTS?

The course requires students to complete weekly assignments, including reading, research, and writing assignments like those required for a three-semester hour graduate-level course. Students must make significant commitments of time to complete assignments. A student's overall grade is made up of four components:

- Weekly discussion forms/ activities: 25%
- Mid-term examination: 25%
- 12-page research paper: 25%
- Final examination: 25%.

DO STUDENTS GET ACE CREDIT OR PDUs?

Course completion offers three semester credit hours in information security or cyber security. The length of the course and in accordance with current certification maintenance guidelines determines the graduate degree category and professional development units per SPēD.

WHAT HAS THE FEEDBACK BEEN LIKE?

The students complete an end of course survey after each completion of a course iteration. Feedback is also compiled along the way. The overall feedback has been very positive and some has changed the course, such as adding additional engagement calls, incorporating knowledge checks, and activities. ■

Learn more or register by visiting the ED 520 page on the CDSE website.

A STRATEGY FOR PROFESSIONALIZATION

Workforce training and professionalization are the cornerstones of success in every industry. Understanding the concepts and principles necessary to perform critical functions and developing the knowledge, skills, and abilities of practitioners ensures effective execution of any objective. Promoting professional development opportunities creates common standards to validate skills and enhance workforce competency; in addition, it can provide information about workforce strengths and weaknesses. Professional development is also a valuable recruitment and retention tool.

By Rebecca Morgan
Senior Advisor
Counter-Insider Threat Program, OUSD(I&S)

The Department of Defense (DOD) has consistently prioritized the development of its workforce to be mission ready and to safeguard and advance vital U.S. national interests. The current National Defense Strategy reinforces this commitment to cultivate diverse talent and train a workforce with the skills and abilities required to creatively solve national security challenges in a complex global environment. In a message to the workforce, Secretary of Defense Lloyd Austin reaffirmed this through his stated priority of "taking care of people" by providing exceptional opportunities for professional development. The Counter-Insider Threat mission supports this priority, and the development of a cadre of professionals is a key element of the DOD Counter-Insider Threat Program Strategy.

Countering the insider threat has always been an integral part of the DOD mission and at the forefront of many disciplines, spanning from counterintelligence to security. However, the paradigm shift initiated by Executive Order 13587 and National Insider Threat Policy and Minimum Standards required a new skill set. With a focus on prevention through proactive risk mitigation and deterrence, sustained multidisciplinary risk management, and the modernization of detection activities through the use of technology, many existing workforce development offerings were insufficient. DOD responded swiftly to this deficiency and, in collaboration with national partners, developed a suite of training, professionalization, education, and awareness opportunities for practitioners of this new discipline and for the general workforce. These partnerships with the National Counterintelligence and Security Center; Defense Counterintelligence and Security Agency; and the Personnel and Security Research Center, among others, have resulted in a robust catalog of offerings for a variety of learning audiences with equities in countering insider threats.

While this collective accomplishment has brought many benefits to the insider threat community, at this point, we almost suffer from an abundance of riches. The multitude of insider threat specific training and educational resources has made it difficult to consistently communicate the availability of offerings, and for DOD Component programs to identify the most essential and beneficial products to develop their personnel and other auxiliary learning audiences. These audiences have expanded to include insider threat practitioners in the defense industrial base and other critical infrastructure sectors whose ability to counter insider threats is essential to national security. Additional audience members include practitioners of Prevention Assistance Response Capability and other prevention activities designed to mitigate acts of workplace violence, sexual assault, and suicide. Individuals in leadership, management, counselor,

guidance, chaplain, and other roles, who are essential to the identification of insider threats and the deployment of sustained risk management strategies, also require specific learning opportunities to facilitate mitigation of insider threats.

In addition, threats posed by trusted insiders, both witting and unwitting, exist in a dynamic risk environment. As such, the skills required to prevent, deter, detect, mitigate, and manage those risks are complex and continually evolving. Programs originally stood up in response to unauthorized disclosure and active shooter incidents must contend with a broad range of threats ranging from espionage, fraud, theft, acts of harm to self or others, foreign and domestic violent extremism, loss or theft of intellectual property or proprietary information, physical and technical sabotage, and more. Evaluating insider risk involves a nuanced understanding of human behavior and a wide range of vulnerabilities and motivations that drive this behavior. In the last few years, there have been increased stressors on the general populace and on the federal workforce, from the global pandemic to economic uncertainty; from a polarized political climate to disruptions from climate change; and from isolation and security factors associated with remote work to an increase in despair exemplified by substance abuse and suicide. These elements are driving factors that, for some trusted insiders, facilitate their transition down a path that might result in negative workforce events. In this changing environment, learning must be recognized as a continuum rather than a one-time event.

The DOD enterprise, and the broader counter-insider threat community in both the public and private sector, require a cadre of professionals with the capability to counter insider threats in this challenging risk landscape. Professionalizing these workforces necessitates the development of content that is both timely and data driven. Incorporating social and behavioral science, statistical, data analytic, and technological research into training, professionalization, education, and awareness offerings will ensure a skilled and adaptive workforce is prepared to counter current and future insider threats.

To support these requirements, the Office of the Under Secretary of Defense for Intelligence and Security's (OUSD(I&S)) Counter-Insider Threat Program has coordinated with stakeholders to develop a new DOD Counter-Insider Threat Training Strategy. Targeted for issuance at the end of 2023, this strategy will clearly define learning audiences and will simplify the professional development path required of our workforce given the abundance of resources. The strategy is aligned with requirements in DOD and national level policy and enables implementation of that policy for DOD programs. It ensures training and professionalization offerings continue to evolve in a manner that addresses the current risk environment and incorporates appropriate research findings. This comprehensive training strategy further enables DOD, U.S. Government, and industry Insider Threat Programs to attain effective mission operations and expands opportunities for professionalization of the Counter-Insider Threat workforce. It ensures timely and strategic materials are deployed to support risk mitigation in emerging threat environments. The strategy engages Counter-Insider Threat practitioners to foster a cohesive community and encourages continuing education. The strategy emphasizes integration with other disciplines, including security, prevention, human resources, ethics, privacy and civil liberties, and others by identifying and supporting new learning audiences and cohorts. It also promotes outreach to facilitate insider threat awareness for identified workforces and the general public.

Over the last decade, the broader insider threat community has matured exponentially – greatly increasing capability to counter insider threats in both the public and private sector. The efforts by DOD and its partners to develop training and professionalization opportunities are an essential factor in the success of this discipline. As we move forward, we recognize that continued partnership with stakeholders – in and out of DOD – will be the most effective means to evolve our capabilities. OUSD(I&S) is excited to continue this process and looks forward to sharing the Strategy and its outcomes with our partners. ■

ABOUT THE AUTHOR

Rebecca Morgan serves as the Senior Advisor to the DOD Counter- Insider Threat Program, Office of the Undersecretary of Defense for Intelligence and Security. She has previously served as the Director, National Insider Threat Task Force; Assistant Director, National Counterintelligence and Security Center; and as a Senior Advisor to the Executive Office of the President. Ms. Morgan has three decades of experience in security and counterintelligence investigations, operations, and analysis and was previously the CDSE curriculum manager for insider threat and counterintelligence.

HIGHLIGHTED

CERTIFICATION PRODUCTS

CERTIFIED CREDIBLE: COUNTER-INSIDER THREAT PROFESSIONALS GET THEIR OWN EXAM

For the first time, professionals fighting insider threats will have an opportunity to prove their expertise through a new certification program starting in June called the Global Counter-Insider Threat (C-InT) Professional Certification Program.

By Kristin P. Jones
University of Maryland
Applied Research Laboratory for
Intelligence and Security

Offered through the University of Maryland Applied Research Laboratory for Intelligence and Security (ARLIS), the certification program will be open to any government or private-sector professional with four years of experience in counter-insider threat roles and who has completed at least 20 hours of specific C-InT training.

William Stephens, who directs the ARLIS insider risk mission area, said, "The purpose of the certification program is to raise the level of performance, standardize language and skills, and validate counter-insider threat practitioners as professionals."

For professionals in this field, the intent is to identify risks, whether they stem from threats, vulnerabilities, or a combination, posed by individuals or groups granted access to sensitive information and systems within an organization. The risk may stem from employees, contractors, vendors, or other trusted partners who have access to valuable data and systems. Insider threats are presented by adversaries intending to work through insiders to steal data, commit sabotage, fraud, espionage, cyber attacks, etc.

The program follows a 12-year federal initiative to strengthen counter-insider threat efforts, starting with Executive Order (EO) 13587, signed by the president in 2011. This executive order mandated the creation of programs in every executive-level department and agency to deter, detect, and mitigate actions by employees presenting a threat to national security. In 2018, the Certified Counter-Insider Threat Professional program was established with the goal of creating a certification program that would establish workforce credibility, foster a professional identity, and catalyze professional development within the Department of Defense and the broader U.S. government.

By 2021, Defense Department leaders and the Certified Counter-Insider Threat Professional Governance Council decided to expand the program globally to public and private sectors.

ABOUT THE AUTHOR

Kristin Patterson Jones is assistant director for strategic communications at the University of Maryland Applied Research Laboratory for Intelligence and Security. ARLIS is the only applied research lab dedicated to multidisciplinary research in the human domain. She has more than 20 years of communications experience in the aerospace and defense industry.

A certification exam was developed and piloted in 2022 and the program was formally launched in March.

The Global Counter-Insider Threat Professional (GCITP) certification exam will be available for on-demand testing and will be exclusively delivered electronically by Pearson VUE in two testing modalities: through any of Pearson VUE's in-person testing centers and through Pearson VUE's live remote proctoring system, which allows candidates to test anywhere from their own devices. When scheduling to take the exam, candidates have the choice between either options at no additional cost to the candidate. For in-person testing, Pearson VUE may meet the needs of most members of the C-InT workforce with their 5,600 locations throughout the United States, Europe, Asia, and the Middle East as well as over 100 U.S. military installations.

"There is no certification program like this anywhere," said Steve Sin, director of Unconventional Weapons and Technology Division at the University of Maryland National Consortium for the Study of Terrorism and Responses to Terrorism (START). "It's the first C-InT certification program developed for a global audience for both public and private professionals."

ARLIS was selected as the home for the certification program because of its applied research in the human domain and ability to tap into capabilities offered through START with proven education and training curricula development and delivery capabilities and expertise in adversary behavior modeling and risk mitigation.

"Receiving certification means the individual is a verified expert, holding significant credibility in C-InT," Sin said. ■

For information about the certification program, visit gcitp.umd.edu or email gcitp@umd.edu. The exam registration fee is $650.

CERTIFIED COUNTER-INSIDER THREAT PROFESSIONAL (CCITP) CERTIFICATION

Interested in becoming CCITP certified? Read our Q&A to learn more about this nationally accredited program and its requirements.

WHAT IS THE CERTIFIED COUNTER-INSIDER THREAT PROFESSIONAL CERTIFICATION PROGRAM?

The Office of the Under Secretary of Defense for Intelligence and Security [(OUSD(I&S)], in partnership with the National Insider Threat Task Force (NITTF), focused on the people-related aspect of the counter-insider threat (C-InT) capability and created two professional certifications. These certifications were developed with maximum participation from across the U.S. Government, resulting in broad applicability across C-InT workforces. The first pilot examinations took place in December 2019 with certifications being first conferred in February 2020.

WHAT IS THE CCITP-FUNDAMENTALS (CCITP-F)?

Measures and assesses whether an individual has the requisite knowledge and skills (K&S) annotated in the CCITP-Essential Body of Knowledge (EBOK) to perform the tasks outlined in the CCITP-Essential Body of Work (EBOW). It was designed with a target population of those personnel working directly in a C-InT program; however, the program is open to anyone who works within or is affiliated with a C-InT program. The examination measures acceptable performance across five topic areas:

1. Policy and directives: 25%
2. Social and behavior science: 10%
3. Researching: 30%

4. & 5. Synthesis & tools and methods: 35%

WHAT ARE THE REQUIREMENTS FOR THE CCITP-F?

The candidate should meet the following requirements: C-InT program affiliation, a minimum of 6 months of experience working in/with a C-InT Program, and a minimum of ten hours of C-InT training. They will be documented in the candidate registration system and must be approved by your organization's Program Manager prior to being allowed to schedule your exam.

HOW LONG IS THE CCITP-F VALID AND WHAT IS REQUIRED FOR RENEWAL?

It is valid two years from conferral, and certificants are required to obtain 100 professional development units (PDUs) over the course of their two-year maintenance cycle to maintain their CCITP-F certification successfully. The 100 PDUs are divided between C-InT specific activities and professional growth activities in the following manner:

- 75 PDUs: C-InT specific
- 25 PDUs: professional growth

WHAT IS THE CCITP-ANALYSIS (CCITP-A)?

CCITP-A establishes a common standard of analytic tradecraft of all who serve and support the C-InT capability. It focuses on the analysis of C-InT information and development of mitigation recommendations. It measures and assesses whether an individual has the requisite K&S annotated in the CCITP-EBOK to perform the tasks outlined in the CCITP-EBOK. The CCITP-A was designed for the target population of those personnel working directly in a C-InT program and performing analysis functions. The examination measures acceptable performance across six topic areas:

1. Policy and directives: 20%
2. Social and behavior science: 10%
3. Researching: 20%

4. & 5. Synthesis & tools and methods: 35%

6. Vulnerabilities assessment and management: 15%

WHAT ARE THE REQUIREMENTS FOR THE CCITP-A?

The candidate should meet the following requirements: Currently hold the CCITP-F certification, C-InT program personnel only, a minimum of 12 months of experience working in/with a C-InT Program, a minimum of 40 hours of analysis-related training, a minimum of 8 hours of user activity monitoring policy and/or tool-related training, and review at least 10 case studies.

HOW LONG IS THE CCITP-A VALID AND WHAT IS REQUIRED FOR RENEWAL?

It is valid three years from conferral, and certificants are required to obtain 100 PDUs over the course of their 3-year maintenance cycle to successfully maintain their CCITP-A certification. The 100 PDUs are divided between C-InT specific activities and professional growth activities in the following manner:

- 50 PDUs: C-InT specific
- 50 PDUs: professional growth

IS THERE TRAINING TO HELP PREPARE FOR THE EXAMINATIONS?

While there are some C-InT courses available across the U.S. government, there are no specific courses specifically tailored to help candidates pass these exams. Candidates are encouraged to review the knowledge domains identified by subject matter experts as being essential knowledge for C-InT. These knowledge domains make up the CCITP-EBOK. The CDSE insider threat toolkit resources, including the EBOK job aid, are good resources to help one prepare for the exams.

HOW DO I REGISTER AND TAKE THE EXAMINATION?

The exams are offered at select times throughout the year, as determined by the CCITP Governance Council and Program Management Office. These windows will be advertised, and application will be allowed for approximately a one-month window, two-months prior to the testing window. During the registration window, candidates must create an account at cint-gsx.learningbuilder.com and complete their profile and registration application. Once submitted, program reviewers will approve or deny a candidate's application based on eligibility and pre-requisite criteria mentioned above. If individuals are approved, they will be notified by or shortly after the end of the registration period and will receive electronic communication with instructions to register with Pearson VUE to schedule their exam. Candidates who are not allotted a seat during the test window will be notified with feedback as to why they were not selected. If time permits and denial was due to an application error, individuals may be able to correct their application; otherwise, they must wait and re-apply during the next registration window.

WHEN WILL I BE CONFERRED?

Candidates who meet all the program's certification requirements, including meeting or exceeding the required score on the relevant exam, will be conferred in the weeks following the conclusion of each testing interval/window.

WHEN WILL I RECEIVE THE CERTIFICATION CREDENTIALS?

Once the conferral process is completed (see previous question), you will receive an email from the CCITP Program Management Office with directions regarding how to access your printable/downloadable certificate and your digital badge. Credentials will be conferred in the weeks following the conclusion of each testing interval/window.

WHAT HAS THE FEEDBACK BEEN LIKE?

After each completion of a course iteration, the students complete an end-of-course survey, compiling feedback along the way. The overall feedback has been very positive, and some of it has resulted in some changes to the course, such as adding additional engagement calls and incorporating knowledge checks and activities. ■

To learn more about CCITP, visit the DOD Intelligence and Security Professional Certification website.

HELPFUL **TOOLS**

INSIDER THREAT PROGRAM OPERATIONS PERSONNEL REQUIREMENTS

The **National Minimum Standards for Insider Threat Programs** gives specific guidance on training mandated for Insider Threat program personnel. The National Minimum Standards for Insider Threat Programs also builds the framework for additional policies: **Department of Defense Directive (DODD) 5205.16** and **32 Code of Federal Regulations (CFR) Part 117 National Industrial Program Operating Manual (NIPSOM) rule.**

WHAT THE NATIONAL INSIDER THREAT POLICY AND THE MINIMUM STANDARDS MEANS FOR INSIDER THREAT PROGRAM PERSONNEL

For those who are assigned to the Insider Threat Program, agency heads shall ensure their personnel are fully trained in:

- Counterintelligence and security fundamentals to include applicable legal issues
- Agency procedures for conducting insider threat response action(s)
- Applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information
- Applicable civil liberties and privacy laws, regulations, and policies
- Investigative referral requirements of Section 811 of the Intelligence Authorization Act for FY 1995 as well as other policy or statutory requirements that require referrals to an internal entity, such as a security office or Office of Inspector General, or external investigative entities, such as the Federal Bureau of Investigation, the Department of Justice, or military investigative services.

WHAT IS DODD 5205.16?

This policy establishes under the DOD the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs in accordance with References (b), (e), (f), and (h).

This means that DOD military and civilian personnel, DOD contractors, and volunteers who have access to DOD resources will be provided with the appropriate training, education, and awareness of the insider threat.

The directive also outlines the role the Defense Counterintelligence and Security Agency (DCSA) will play to achieve these goals by:

- Incorporating insider threat education and awareness material into DCSA security education and training programs provided to DOD components and cleared DOD contractors
- Providing oversight, training, and guidance in accordance with DODD 5105.42 to cleared contractors regarding insider threats
- Providing a representative to departmental and interagency forums engaged in countering insider threats

WHAT IS SECTION 117.12 OF 32 CFR PART 117 ?

This policy defines the requirements for how insider threat training is conducted. Specifically, contractor Insider Threat Program personnel, including the contractor designated Insider Threat Program senior official, must be trained in:

- Counterintelligence and security fundamentals, including applicable legal issues
- Procedures for conducting Insider Threat response actions
- Applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information
- Applicable legal, civil liberties, and privacy policies
- Counterintelligence and security reporting requirements, as applicable

The Center for the Development of Security Excellence (CDSE) offers two curricula that meet these requirements. The curricula are made up of various e-learning courses designed to equip students with the knowledge, skills, and abilities required to conduct their duties. **There** is no clearance requirement to enroll or participate in the curricula.

INSIDER THREAT PROGRAM OPERATIONS PERSONNEL CURRICULUM

This curriculum provides specialized training for analysts and other operations personnel working in insider threat programs within DOD components, federal agencies, and industry. This curriculum is composed of 12 e-learning courses and takes approximately 22.75 hours.

Target Audience:
DOD military, civilian, and contractor security professionals and practitioners responsible for protecting and maintaining an insider threat program for their organization.

Courses:

- **PS113.16:** Introduction to Personnel Security
- **IF130.16:** Unauthorized Disclosure (UD) of Classified Information and Controlled Unclassified Information (CUI)
- **CI116.16:** Counterintelligence Awareness and Reporting for DOD Employees
- **CS200.16:** Continuous Monitoring
- **INT210.16:** Insider Threat Mitigation Responses
- **INT220.16:** Preserving Investigative and Operational Viability in Insider Threat Referrals
- **INT230.16:** Insider Threat Indicators in Records Checks
- **GS105.16:** Active Shooter Awareness Short
- **INT 250.16:** Insider Threat Critical Thinking for Analysts
- **INT 260.16:** Insider Threat Privacy and Civil Liberties
- **INT 280.16:** Cyber Insider Threat
- **INT 290.16:** Behavior Science in Insider Threat

INSIDER THREAT PROGRAM MANAGEMENT PERSONNEL CURRICULUM

This curriculum provides specialized training for personnel managing an insider threat program. This curriculum is composed of 13 e-learning courses and takes approximately 24.25 hours.

Target Audience:
DOD, industry, and federal agency professionals responsible for managing an insider threat program for their organization.

Courses:

- **PS113.16:** Introduction to Personnel Security
- **IF130.16:** Unauthorized Disclosure (UD) of Classified Information and Controlled Unclassified Information (CUI)
- **CI116.16:** Counterintelligence Awareness and Reporting for DOD Employees
- **INT201.16:** Developing a Multidisciplinary Capability for Insider Threat Course
- **GS105.16:** Active Shooter Awareness Short
- **INT210.16:** Insider Threat Mitigation Responses Course
- **INT220.16:** Preserving Investigative and Operational Viability in Insider Threat Referrals Course
- **INT240.16:** Insider Threat Basic HUB Operations
- **INT260.16:** Insider Threat Privacy and Civil Liberties
- **INT270.16:** Maximizing Organizational Trust
- **INT280.16:** Cyber Insider Threat Course
- **INT290.16:** Behavioral Science in Insider Threat
- **INT122.16:** Establishing an Insider Threat Program Course

HUB ANALYST TRAINING ROADMAP

The Counter-Insider Threat (C-InT) mission space continues to evolve. There is growing need for a comprehensive professionalization program to better equip the C-InT workforce with the necessary skillsets to deter, detect, and mitigate the threats trusted insiders pose to national security, critical infrastructure, and our private sector partners. To support this effort, The Threat Lab, a division of the Defense Personnel and Security Research Center (PERSEREC), created a **professionalization Road Map for C-InT Analysts** that helps to elevate the role from a series of tasks to a profession of its own.

Originally published by ThreatLab

AUTHORS:
Northrop Grumman Defense Systems: Lorien Megill and Mario Ruiz
Global Skills X-Change: Caitlyn Foley, Amanda Boelke, Slaton Lucero, and Marisa Peyton
Defense Personnel and Security Research Center: Stephanie Jaros and Leissa Nelson

The Road Map defines the role of the C-InT Analyst in a C-InT Hub, the core knowledge that they need, and establishes expectations for professional advancement. The Road Map defines seven core competencies and the associated knowledge and skill areas needed to advance from novice Hub Analyst to the advanced level.

A good training plan boosts employees' competencies, development, and helps them be more effective in their roles. Studies show that over 40% of employees quit their jobs because of a lack of career development, and training is vital for development. A well-designed employee-training plan also makes for a happier, more productive workforce. No matter the industry, filling the gaps in your employees' professional knowledge is essential to keeping them productive and fulfilled.

This article lays out one proposed Training Plan for advancing and tracking the development of the skills needed by novice C-InT Hub Analysts. It is by no means the only way to achieve this goal, but it does address available training resources for all seven core competencies and disciplines involved in an effective C-INT program. **This training can advance a Hub Analyst's skillset from a novice level to and intermediate level in just a two-year period.**

SPONSORS:
Department of Defense PERSEREC (Defense Personnel and Security Research Center), part of the Office of People Analytics (OPA)
National Insider Threat Task Force
Department of Defense Counter-Insider Threat Program

INTRODUCTION

As the Counter-Insider Threat (C-InT) mission space continues to evolve, there is a need for a comprehensive professionalization program to better equip the C-InT workforce with the necessary skillsets to deter, detect, and mitigate the threats trusted insiders pose to national security, critical infrastructure, and our private sector partners.

To support this effort, the National Insider Threat Task Force (NITTF) asked The Threat Lab, a division of the Defense Personnel and Security Research Center (PERSEREC), to create a professionalization Road Map for C-InT Analysts that will help elevate the role from a series of tasks to a profession of its own.

The finished Road Map is designed to:

- Define the role of the C-InT Analyst in a C-InT Hub
- Define a core knowledge base that support's an organization's understanding of the C-InT Analyst's role
- Establish expectations for foundational knowledge and professional advancement.

METHOD

We developed and validated the content of this Road Map by reviewing existing policy and professionalization materials and conducting interviews with subject matter experts (SMEs) from organizations across the federal government and cleared industry partners. We began our research by reviewing publicly-available C-InT policies and program documentation published by the United States government.

Second, we held nine focus groups with 19 SMEs in March 2021. These focus groups included government and private sector SMEs from nine organizations identified as model programs by the OUSD(I&S) DOD Counter-Insider Threat Program. OUSD(I&S) defined model programs as those with advanced capabilities in one or more C-InT lines of effort (i.e., pillars) and/or fully operational programs with more structured systems for training and developing C-InT Analysts. To maximize candor, we promised SMEs we would not reference their names or organizations in the final deliverable. Focus groups lasted up to one hour and focused on a list of brainstorming questions that we sent SMEs ahead of time. We provided field notes to each SME after the focus group for review and revision to ensure accuracy.

We used the results of the document review and SME interviews to 1) refine the key tasks and competencies, 2) define the roles and responsibilities of three levels of C-InT Analyst, and 3) identify the education/training, experience, and exposure required to advance from one level to the next. We used the following definitions for these requirements:

- **Education/Training:** Learning opportunities, such as on-the-job training (OJT) or formal/classroom training, that teach C-InT Analysts the necessary knowledge and skills to fulfill their role
- **Experience:** The suggested amount of time it takes an individual working in a C-InT Program to learn how to successfully perform the tasks needed to transition to the next level of C-InT Analyst and the type of tasks performed during that time
- **Exposure:** Activities or opportunities that provide C-InT Analysts the chance to learn about the full breadth of the C-InT mission space including inquiry types, fields related to C-InT, and inquiry study outcomes

In addition to the focus groups, we conducted semi-structured interviews. These interviews were intended to refine the education, experience, and exposure identified in the early phases of the work and to define the minimum proficiency levels (i.e., level of performance) at which C-InT Analysts must perform each key C-InT Analyst task and understand each key C-InT competency. We conducted the interviews with five individuals from the initial nine model programs. Telephone interviews lasted up to ninety minutes. After each interview, we provided field notes to the SMEs for review and revision to ensure accuracy. We then aggregated and analyzed those field notes.

RESULTS

Using the results of the document review, focus groups, and interviews, we developed a list of high-level, overarching functions meant to cover the majority of a C-InT Analyst's position, which we identified as the key C-InT Analyst tasks. We also developed a list of high-level, overarching competencies meant to cover the majority of the knowledge and skills needed by C-InT Analysts, which we identified as key Analyst competencies. The knowledge and skill areas that make up each competency are shown in Table 1.

TABLE 1: SEVEN C-INT ANALYST KEY COMPETENCIES

Competency	Knowledge and/or Skill Areas	
C1. C-INT Fundamentals	▪ C-InT policies and directives ▪ Privacy and civil liberties protections ▪ Risk Management Framework (RMF)	▪ C-InT pillars ▪ C-InT Program/Hub mission, resources, and policies
C2. Information Collection and Validation	▪ Building collaborative relationships with pillar ▪ experts or outside experts ▪ Source identification ▪ Information source research ▪ Evaluation and guidance of information collection ▪ Data collection strategies	▪ Outreach strategies ▪ Identifying gaps in data ▪ Databases and data feeds ▪ Information requests ▪ Data validation/evaluation ▪ Referral triage ▪ Monitoring and tracking data feeds
C3. Data Integration and Analysis	▪ Data aggregation ▪ Data normalization ▪ Baseline identification ▪ Contextualizing behavior to form a baseline ▪ Risk-scoring technologies	▪ Anomalous behavior identification ▪ Whether anomalous behavior meets thresholds/indicators ▪ Longitudinal analysis ▪ Identifying gaps in data
C4. Critical Thinking	▪ Intellectual standards (interpreting, analyzing, etc.) ▪ Analytic methodologies and tools	▪ Identifying cognitive limitations (e.g., cognitive biases) ▪ Discernment of biases ▪ Proposing alternative hypotheses
C5. Response and Mitigation	▪ Individual mitigation strategies ▪ Organizational mitigation strategies ▪ Procedures for determining/conducting insider threat response actions	▪ Measures used to reduce unauthorized disclosure
C6. Inquiry Management and Information Protections	▪ Inquiry lifecycle ▪ Investigative and operational viability ▪ Information protection/safeguarding information ▪ Documenting insider threat matters ▪ Digital asset records management ▪ Investigative referral requirements; development of referrals to other departments/agencies	▪ Case management tools used to ensure the integrity and effectiveness of the inquiry and response processes ▪ Understanding the appropriate officials to consult for authoritative compliance (e.g., legal, privacy and civil liberties, agency policy, etc.)
C7. Information Sharing and Dissemination	▪ Developing reports following analytic tradecraft standards ▪ Intelligence Community analytic standards	▪ Demonstrating customer relevance and addressing implications ▪ Requesting/responding to customer feedback

We also identified the education, experience, and exposure needed to progress from one level of C-InT Analyst to the next and identified existing available training and resources.

In addition to the information included in the Road Map, we used the review of references and the focus groups to develop definitions for three levels of Analyst: Beginner, Intermediate, and Advanced. Beginner Analysts can perform specific, defined tasks autonomously, while more Intermediate and Advanced Analysts review and supervise all of their work. Intermediate Analysts can work most inquiries autonomously and follow the inquiries management process. Intermediate Analysts may require some assistance from Advanced Analysts to complete more novel or complex inquiries. Advanced Analysts provide oversight and/or guidance to other C-InT Analysts, perform strategic analyses, and manage both internal and external data sources to complete analyses. Full definitions of each level of C-InT Analyst are shown in Table 2.

TABLE 2: C-INT ANALYST DEFINITIONS

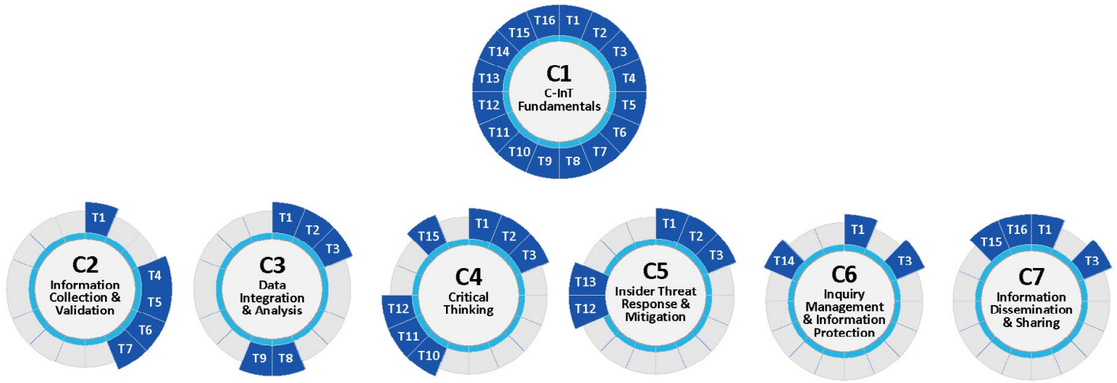
Title	Knowledge and/or Skill Areas
Beginner Analyst	Beginner Analysts have previous experience in a C-InT-related field (e.g., Human Resources, Counterintelligence, Security, etc.) or have applied the C-InT Analyst core competencies in a different role/job setting. These individuals may have minimal experience working directly in or in support of a C-InT Program. These individuals are focused on: learning the inquiry management process, how and when to use available databases, and specific organizational procedures through on-the-job training (OJT); completing analysis courses; and practicing writing and briefing skills. These individuals collaborate with more experienced Analysts to learn the process and develop the foundational knowledge needed to lead an inquiry. These individuals triage reports/tips, begin collecting information from data sources, and begin the initial data analysis to form the big picture. These individuals are able to perform specific, defined tasks autonomously, but Intermediate and Advanced Analysts review and supervise all of their work.
Intermediate Analyst	Intermediate Analysts have experience working directly in a C-InT Program. These individuals have received formal training in C-InT analysis and have received on-the-job training (OJT) to grow their knowledge and understanding of the various disciplines that make up the C-InT mission. These individuals use their knowledge to collect, validate, and aggregate data to provide stakeholders with a holistic perspective of a subject's potential risk indicators (PRIs). These individuals work collaboratively with all other team members to identify and fill gaps in their work product. While able to work most inquiries autonomously and follow the inquiry management process, these individuals may require some assistance from advanced C-InT Analysts to complete more novel or complex inquiries. These individuals are beginning to learn how to develop mitigation recommendations.
Advanced Analyst	Advanced Analysts have extensive experience working directly in a C-InT Program. These individuals have received formal training in C-InT analysis, are responsible for the most complex or high threat inquiries, work closely with other Analysts to assist as needed, collaborate with various stakeholders, and draw connections between seemingly disparate information. These individuals have a deeper understanding of the tools, techniques, and processes utilized by experts in related fields (e.g., psychology, threat assessment, counterintelligence) and when to involve those experts. They take a more proactive approach to identify new alerts/flags and develop mitigation responses to their inquiries. Work activities for these individuals may include: providing oversight and/or guidance to other C-InT Analysts, performing strategic analyses, and managing both internal and external data sources to complete analyses. These individuals may provide mitigation recommendations to internal and external stakeholders and leadership in a way that makes sense to non-C-InT professionals or, in rare inquiries involving imminent danger, take action to implement some mitigation responses.

The information and definitions depicted in the Road Map represent the aggregated results of the policy review and SME interviews. We present three data visualizations, described as follows.

- Overview of Key C-InT Analyst Tasks and Competencies: This visualization describes the key tasks and competencies and shows how the competencies are linked to each task.
- Expected Proficiency of Each Competency at Each Level of a C-InT Analyst's Career: This visualization rates each competency for the Beginner, Intermediate, and Advanced Analyst using a five-point proficiency scale.
- How to Transition from Beginner to Intermediate Analyst and Intermediate to Advanced Analyst: This visualization lists the education/training, experience, and exposure that help an Analyst advance along their career path.

Taken together, we encourage C-InT professionals to use these data visualizations to target areas for advancement and development. We encourage C-InT programs to use these data visualizations to determine selection criteria, to advance their people, and to identify relevant training.

KEY C-INT ANALYST TASKS AND COMPETENCIES



Task 1
Comply with and stay current on relevant C-InT and other regulations, laws, policies and directives.

Task 2
Apply C-InT Discipline Knowledge to the analytic process to contextualize behavior and identify concerning behavior.

Task 3
Apply agency and organizational potential risk indicators and/or reporting thresholds to all analytic and inquiry management processes.

Task 4
Establish collaborative relationships with internal/ external partners and stakeholders to facilitate information gathering and inquiry/investigation processes, mitigate bias, and support the overall C-InT mission.

Task 5
Receive and/or validate potential InT information to identify resource needs for collection.

Task 6
Gather information relevant to the potential risk indicators presented by an individual using multiple data sources.

Task 7
Identify gaps in the content of gathered information and determine any gaps in information sources.

Task 8
Integrate collected information to identify a baseline set of behaviors for an individual.

Task 9
Identify and flag anomalous activity using data integration methodologies and advanced analytics to contextualize an individual's behavior.

Task 10
Evaluate, integrate, analyze, and interpret information using structured analytic techniques.

Task 11
Evaluate and prioritize alternatives and assess similarities and differences in data to develop findings and conclusions.

Task 12
Determine whether an individual is a potential insider threat and, if applicable, recommend tailored mitigation strategies, either individual or organizational.

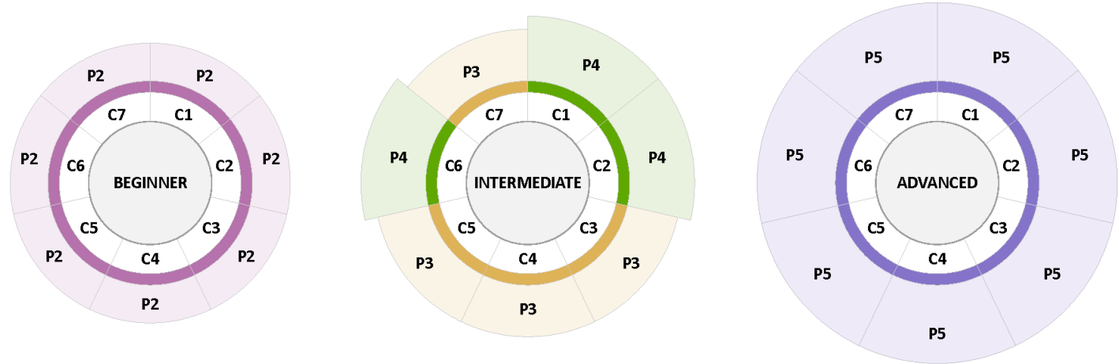
Task 13
Review insider threat indicators and recommend updates to organizational trigger policies based on environmental and/or situational changes, as needed.

Task 14
Employ case management principles and tools to ensure the integrity and effectiveness of the insider threat inquiry and response processes.

Task 15
Report and brief findings to internal/ external leadership, and ensure reporting follows analytic standards, demonstrates stakeholder relevance, and addresses implications.

Task 16
Request and respond to stakeholder comments and/or feedback.

EXPECTED PROFICIENCY OF EACH COMPETENCY AT EACH LEVEL OF A C-INT ANALYST'S CAREER



P1: Fundamental Awareness *

Basic Knowledge
Focus: Learning
Individuals at this level:
- Have a common knowledge or understanding of the basics

P2: Novice

Limited Experience
Focus: Development through training
Individuals at this level:
- Understand relevant terminology, concepts, principles, and issues
- Are expected to need help completing work

P3: Intermediate

Practical Application
Focus: Application and enhancement
Individuals at this level:
- Understand the application of and implication of changes to relevant processes, policies, and procedures

P4: Advanced

Applied Theory
Focus: Coaching others
Individuals at this level:
- Are "people to ask" when difficult questions arise
- Offer practical ideas on process improvements
- Develop reference and resource materials

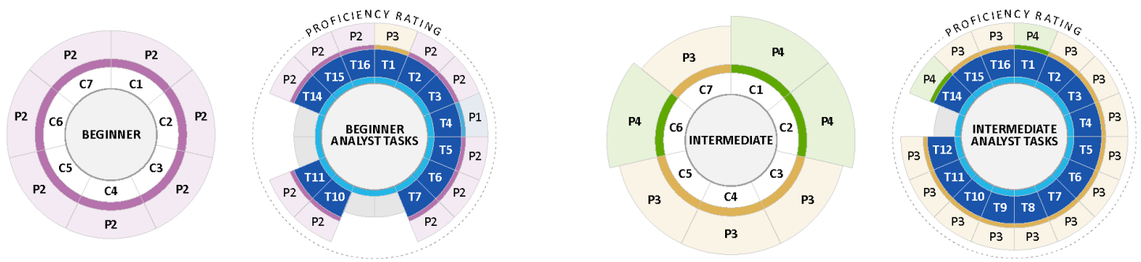
P5: Expert

Recognized Authority
Focus: C-InT Program strategy and development
Individuals at this level:
- Provide guidance, troubleshoot, and answer general and specific C-InT questions
- Are able to present relevant process elements and issues in relation to organizational issues and trends

C1: C-InT Fundamentals
C2: Information Collection & Validation
C3: Data Integration & Analysis
C4: Critical Thinking
C5: Insider Threat Response & Mitigation
C6: Inquiry Management & Information Protection
C7: Information Dissemination & Sharing

** The scale provided to the SMEs included P1, but their average ratings did not identify P1 for any competencies, indicating that even Beginner Analysts enter the field with some relevant background knowledge.*

HOW TO TRANSITION FROM BEGINNER TO INTERMEDIATE ANALYST



Education/Training:

- 40 hours of hybrid C-InT Program training; formats may include formal training and on-the-job training (OJT), covering:
  - C-InT 101 (e.g., what is C-InT, what is a hub, pathway of an insider threat, C-InT pillars)
  - Policy & directives
  - Organizational hub/program structure & procedures
  - Social & behavioral science fundamentals
  - C-InT research, information collection, & validation
  - Vulnerabilities assessment & management
- 100 hours of OJT, topics may include:
  - Holistic, whole-person perspective
  - Organizational policies, procedures, and positioning
  - Organization-specific data sources and pulling data for inquiries
  - Inquiry management knowledge
  - InT terminology
  - Writing and briefing standards
- Additional formal training – examples listed under "training/ resources" below

Experience:

- Experience working in a C-InT Program performing tasks such as:
  - Triaging reports/alerts/tips
  - Managing autonomously the lifecycle of three or more common inquiries types (e.g., low threat, low risk)
  - Identifying connections between inquiries and new information
  - Identifying information gaps and data collection needs

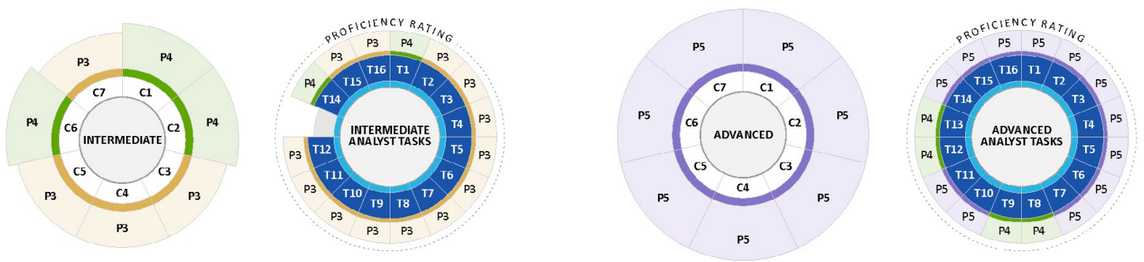
Exposure:

- Collaborate with Intermediate and Advanced Analysts to learn the holistic perspective and how to develop mitigation responses
- Establish collaborative relationships with internal and external partners, stakeholders, and subject matter experts (e.g., behavioral psychologists and data scientists)
- Review case studies covering the breadth of InT event types

Training/Resources to Help Transition from Beginner to Intermediate

- **CDSE, INT311.CU:** Insider Threat Program Operations Personnel Program
- **CDSE, INT101.16:** Insider Threat Awareness Course
- **CDSE, INT240.16:** Insider Threat Basic Hub Operations
- **CDSE, INT250.16:** Critical Thinking for Insider Threat Analysts
- **CDSE, INT260.16:** Insider Threat Privacy and Civil Liberties
- **CDSE, INT311.CU:** Insider Threat Program Operations Personnel Program
- **CDSE:** Insider Threat Resources (e.g., Job Aids, Webinars)
- Certified Counter-Insider Threat Professional-Fundamentals (CCITP-F) Certification
- Counter-Insider Threat Analyst Basic Tradecraft Primer
- Insider Threat Detection Analysis Course (ITDAC)
- Insider Threat Analyst Workbook
- Insider Threat Mitigation Guide
- **NITTF:** Additional Insider Threat Resources
- **NITTF:** Directives & Advisories
- 2017 NITTF Insider Threat Guide
- Insider Threat Training Module (External Learning)
- **NITTF:** Maturity Framework
- **The Threat Lab:** Introduction to Behavioral Threat Assessment
- Threat Assessment Glossary (University of Nebraska, Lincoln)
- A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis

HOW TO TRANSITION FROM INTERMEDIATE TO ADVANCED ANALYST



Education/Training:

- 40+ hours of training in C-InT Analytic Methodology and Techniques; topics may include:
  - Identifying relevant events & connections
  - Autonomously writing concise analytic finding reports
  - Identifying which events/ triggers require immediate action & which allow more time for research
  - Introducing creativity into the analysis process (e.g., developing new intelligence, identifying previously unused information, imagining previously unidentified threats, introducing new tools & techniques)
- Discipline-specific training (e.g., UAM, law enforcement, social and behavioral science, human resources)
  Note: The exact number of hours required per discipline is dependent on the individual InT Program's needs and environment
- On-the-job training in program management
- Additional formal training – examples listed under "training/ resources" below

Experience:

- Experience working in a C-InT Program performing tasks such as:
  - Using internal and external data sources to assess threats
  - Writing and briefing inquiry analysis, results, and mitigation responses to higher level officials
  - Mentoring other C-InT Analysts
  - Applying the holistic perspective to inquiries
  - Modifying existing flags/alerts to better identify "true" threats

Exposure:

- Brief case studies covering the breadth of InT event types
- Obtain C-InT discipline-specific certifications based on work (e.g., Senior Cybersecurity certification, Personnel Security certifications, Certified Threat Manager certification)
- Work to obtain SEI CERT Insider Threat Program Manager certificate

Training/Resources to Help Transition from Intermediate to Advanced

- **CDSE, INT290.16:** Behavioral Science in Insider Threat
- **CDSE, INT280.16:** Cyber Insider Threat
- **CDSE, INT201.16:** Developing a Multidisciplinary Insider Threat Capability
- **CDSE, INT122.16:** Establishing an Insider Threat Program for Your Organization
- **CDSE, INT210.16:** Insider Threat Mitigation Responses
- **CDSE, INT312.CU:** Insider Threat Program Management Personnel Curriculum
- **CDSE, INT220.16:** Preserving Investigative and Operational Viability in Insider Threat
- Certified Counter-Insider Threat Professional-Analysis (CCITP-A) Certification
- Cyber Intelligence Tradecraft Report (Carnegie Mellon University)
- **NITTF:** Additional Insider Threat Resources
- **NITTF:** Directives and Advisories
- Privacy and Civil Liberties Refresher Training
- **Structured Professional Judgment (SPJ) Tools:** A Reference Guide for Counter-Insider Threat (C-InT) Hubs

C-INT HUB ANALYST TRAINING PLAN
YEAR: ONE • TOTAL TIME: 54 HOURS

Competencies	First Quarter *13.75 hours*	Second Quarter *12.75 hours*	Third Quarter *13.5 hours*	Fourth Quarter *14.0 hours*
C1. C-INT Fundamentals	**CDSE eLearn:** INT240: Basic Hub Operations *1 hour*			
	CDSE eLearn: INT122: Establishing an Insider Threat Program for Your Organization *1 hour*			
	CDSE eLearn: INT201: Developing a Multidisciplinary Insider Threat Capability *1.5 hours*			
	Supplemental Reading: Executive Order 13587: Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information National Insider Threat Policy and Minimum Standards			
C2. Information Collection and Validation		**CDSE eLearn:** INT270: Maximizing Organizational Trust *1 hour*	**CDSE eLearn:** INT230: Insider Threat Records Checks *1.5 hours*	

Competencies	First Quarter *13.75 hours*	Second Quarter *12.75 hours*	Third Quarter *13.5 hours*	Fourth Quarter *14.0 hours*
C2. Information Collection and Validation *(cont.)*		**CDSE eLearn:** INT220: Preserving Investigative and Operational Viability in Insider Threat *1 hour*	**CDSE eLearn:** CS200: Continuous Monitoring Course *1.5 hours*	
		CDSE eLearn: INT280: Cyber Insider Threat *0.5 hour*		
C3. Data Integration and Analysis		**Video Short:** HR and Insider Threat (usalearning.gov) *0.25 hour*	**CDSE eLearn:** INT290: Behavioral Science *0.5 hour*	
C4. Critical Thinking				**CDSE eLearn:** INT250: Critical Thinking *1.5 hours*
C5. Response and Mitigation	**Video Short:** Active Shooter Awareness (usalearning.gov) *0.25 hour*			**CDSE eLearn:** INT 210: Insider Threat Mitigation Responses *1 hour*
C6. Inquiry Management and Information Protection				**CDSE eLearn:** INT260: Insider Threat Privacy and Civil Liberties *1.5 hours*
C7. Information Sharing and Dissemination	Additional Training/ Reading from Resource List and Review of Case Studies *10 hours*	Additional Training/ Reading from Resource List and Review of Case Studies *10 hours*	Additional Training/ Reading from Resource List and Review of Case Studies *10 hours*	Additional Training/ Reading from Resource List and Review of Case Studies *10 hours*

C-INT HUB ANALYST TRAINING PLAN
YEAR: TWO • TOTAL TIME: 82.25 HOURS

Competencies	First Quarter *16.75 hours*	Second Quarter *12.0 hours*	Third Quarter *13.5 hours*	Fourth Quarter *40.0 hours*
C1. C-INT Fundamentals	**CDSE eLearn:** CS100.CU: Risk Management Framework (RMF) *4.5 hours*	**CDSE eLearn:** CI116.06: Counterintelligence Awareness and Reporting Course for DOD Employees *1 hour*	**Supplemental Reading:** Unauthorized Disclosure Security Professional Briefing PPT (live.com) *0.5 hour*	
C2. Information Collection and Validation	**Video Short:** Data Quality and Insider Threat Programs: Why It Matters (cdse.edu) *0.25 hour*			Virtual Insider Threat Detection Analysis Course *40 hours*
C3. Data Integration and Analysis				
C4. Critical Thinking			**4-Part Video Series:** Insider Threat Vigilance, Season 2 *1 hour*	
C5. Response and Mitigation		**4-Part Video Series:** Insider Threat Vigilance, Season 1 *1 hour*	Insider Threat Mitigation Workshop (CISA) *2 hours*	
C6. Inquiry Management and Information Protection	**CDSE eLearning:** DS-IF101.06: Identifying and Safeguarding Personally Identifiable Information (PII) *1 hour*			
C7. Information Sharing and Dissemination	**Presentation:** SEAD 3: Awareness Briefing (dni.gov) *1 hour*			
	Additional Training/ Reading from Resource List and Review of Case Studies *10 hours*	Additional Training/ Reading from Resource List and Review of Case Studies *10 hours*	Additional Training/ Reading from Resource List and Review of Case Studies *10 hours*	Additional Training/ Reading from Resource List and Review of Case Studies *10 hours*

DIRECTORY OF RESOURCES

The following is a compilation of products and services developed across the federal government and private sectors that support counter-insider threat professionalization. Most education and training resources will award professional development units (PDUs) to assist in maintenance of certifications.

Courses with an asterisk (*) indicate resources that are available to a USG audience only or may require fees.

EDUCATION (GRADUATE LEVEL)

Marymount University:

FLP 576: Foundations of Insider Threat*

Center for Development of Security Excellence (CDSE):

ED 504: Understanding Adversaries and Threats to the United States and the DOD

ED 520: Foundations of Insider Threat Management

Applied Research Laboratory for Intelligence and Security (ARLIS), University of Maryland

BSST650: Foundations of Insider Risk Management and Mitigation*

BSST651: The Psychology of Malicious Insiders*

BSST652: Managing Insider Threat Activities*

BSST653: Investigative Thinking, Analysis, and Decision-Making in Insider Risk Management and Mitigation*

For more information, visit the University of Maryland website

CERTIFICATION PROGRAMS

Department of Defense

Certified Counter-Insider Threat Professional (CCITP) Program

For USG personnel

University of Maryland

Global Counter-Insider Threat Professional (GCITP) Program*

For industry personnel

TRAINING (E-LEARNING / INSTRUCTOR-LED / VIRTUAL INSTRUCTOR-LED)

Center for Development of Security Excellence (CDSE):

C-INT FUNDAMENTALS

CI020: Counterintelligence Concerns for National Security Adjudicators

CI102: Supply Chain Threat Awareness

CI112: Counterintelligence Awareness and Security Brief

CI116: Counterintelligence Awareness and Reporting for DOD

CI117: Protecting Assets in the NISP

CS200: Continuous Monitoring

IF130: Unauthorized Disclosure (UD) of Classified Information and Controlled Unclassified Information (CUI)

INT101: Insider Threat Awareness

INT260: Insider Threat Privacy and Civil Liberties

INT270: Maximizing Organizational Trust

INT280: Cyber Insider Threat

INT290: Behavioral Science in Insider Threat

CRITICAL THINKING

INT250: Critical Thinking for Insider Threat Analysts

INFORMATION COLLECTION AND VALIDATION

INT122: Establishing an Insider Threat Program for Your Organization

INT201: Developing a Multidisciplinary Insider Threat Capability

INT230: Insider Threat Records Checks

RESPONSE AND MITIGATION

INT210: Insider Threat Mitigation Responses

INT240: Insider Threat Basic Hub Operations

INQUIRY MANAGEMENT AND INFORMATION PROTECTION

INT220: Preserving Investigative and Operational Viability in Insider Threat

ALL AREAS OF COMPETENCY

Insider Threat Detection Analysis

FEMA Emergency Management Institute

C-INT FUNDAMENTALS

IS-906: Workplace Security Awareness

IS-907: Active Shooter: What You Can Do

IS-914: Surveillance Awareness: What You Can Do

IS-915: Protecting Critical Infrastructure Against Insider Threats

IS-916: Critical Infrastructure Security: Theft and Diversion – What You Can Do

Carnegie Mellon University

C-INT FUNDAMENTALS

Building an Insider Threat Program*

Insider Threat Awareness Training*

Insider Threat Program Manager: Implementation and Operation*

Overview of Insider Threat Concepts and Activities*

INFORMATION COLLECTION AND VALIDATION

Insider Threat Analyst*

RESPONSE AND MITIGATION

Insider Threat Program Evaluator*

Insider Threat Vulnerability Assessor Training*

Defense Personnel and Security Research Center (PERSEREC)

C-INT FUNDAMENTALS

A Culture of Ethics

For more information, email dodhra.dodc-mb.dmdc.mbx.threat-lab@mail.mil

Cybersecurity & Infrastructure Security Agency (CISA)

C-INT FUNDAMENTALS

Insider Threat Mitigation Workshop

National Counterintelligence and Security Center (NCSC)

C-INT FUNDAMENTALS

Insider Threat Training

Mental Wellness Training

ALL AREAS OF COMPETENCY

Insider Threat Hub Operations

Joint Knowledge Online (JKO)

C-INT FUNDAMENTALS

Operations Security

Organizational Socialization

Preventing Workplace Violence for Employees

Preventing Workplace Violence for Supervisors

Violence: A Preventable Public Health Issue

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

Have a question about accessing or taking a course, viewing your transcript, or are you experiencing a technical difficulty or other issue related to the STEPP learning management system?

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

Have questions or concerns about CDSE accessibility? Email cdseaccessibility@mail.mil.

CERTIFICATION DIVISION/SPĒD PROJECT MANAGEMENT OFFICE

Have a question related to SPēD Certification? Email dcsa.spedcert@mail.mil.

EDUCATION DIVISION

Have a question about CDSE's curriculum of advanced and graduate courses or education certificates? Email dcsa.cdseeducation@mail.mil.

TRAINING DIVISION

Have a question related to a specific subject matter like counterintelligence, insider threat, or something else? Email dcsa.cdsetraining@mail.mil.

WEBINARS

Have a question about logging into a webinar or conference? Email dcsa.cdsewebinars@mail.mil.

WEBMASTER

Have a suggestion on how to improve or enhance the CDSE website or would you like to report a broken link or other issue with a page? Email dcsa.cdseweb@mail.mil.

STILL NOT SURE WHOM TO CONTACT?

Email dcsa.ncr.dcsa-cdse.mbx.cdse-front-office@mail.mil.

AIRE is published by the Defense Counterintelligence and Security Agency (DCSA) Center for Development of Security Excellence (CDSE) Insider Threat Division.

CDSE

THECDSE

CDSE

CDSE