DoD Insider Threat Program

– Best Practices –

2.1 Training for InT Analysts

Rev 2

05/24/2017

The Under Secretary of Defense for Intelligence is the Senior Official for Insider Threat

Do you have any questions, comments, or concerns on this topic or others?
Would you like to add your component to this Best Practices Edition?

If so, please contact the DoD Insider Threat Program at
osd.pentagon.ousd-intel.mbx.dod-insiderthreatprogram@mail.mil

We look forward to updating and revising this edition, by adding other participants.

NOTE: The Best Practices series will deliberately be anonymized so that responses are not attributed to a participating Component with exception to the DoD Insider Threat Management Analysis Center (DITMAC), the Center for Development of Security Excellence (CDSE), and the National Insider Threat Task Force (NITTF). The information in this booklet is offered as guidance. It does not convey a task or directive. Each Component conforms to multiple and varying authorities. As such, each Component needs to confer with their Office of General Counsel (OGC) to verify their procedures conform to legal pronouncements.

Purpose:

The DoD Insider Threat Program has compiled data and information from several selected DoD Components that can offer field tested procedures which have produced credible results. These methods, techniques, and professional procedures are offered to Components to assist in their efforts to improve their respective Insider Threat Program (InTP). All best practices are informational, and individual programs should ensure any implementation actions are in compliance with their Office of General Counsel (OGC) and organizational policies before implementation.

Description:

This edition addresses questions pertaining to how Components have trained the analysis positions embedded in the Hubs of their respective InTP. There are a total of 12 questions that were posed to 5 Components. Non Components (DITMAC, CDSE, and NITTF) participated as well, conveying their role in providing analysis training throughout the enterprise.

Acronyms:

CI	Counterintelligence	**IAM**	Info Sec Assessment Methodology	**PII**	Personally Identifiable Information
COTR	Contracting Officer's Technical Representative	**IAT**	Information Assurance Training	**PD**	Position Description
DSoS	DITMAC System of Systems	**IC**	Intelligence Community	**PM**	Program Manager
DSS	Defense Security Service	**InT**	Insider Threat	**SORN**	System of Records Notice
FY	Fiscal Year	**InTP**	Insider Threat Program	**SOP**	Standard Operating Procedure
HR	Human Resources	**LE**	Law Enforcement	**UAM**	User Activity Monitoring
IAA	Information Assurance Awareness	**OPSEC**	Operations Security	**USG**	United States Government

Table of Contents

NOTE: Since DITMAC has a unique mission and is not a Component InT hub, some of these questions do not apply to them and they have been noted in those instances. Their responses still add value to the Best Practices series.

Q1. Does your organization have an established specialized/focused training program for Hub analysts or do you leverage outside training?

DITMAC

The DITMAC established a training curriculum for all DITMAC analysts leveraging a variety of external training sources, to include several courses offered by CDSE, other USG providers (Director of National Intelligence (DNI), Defense Intelligence Agency (DIA)) and commercial providers. Additionally, to supplement formal training, DITMAC conducts internal training modules, leveraging expertise organic to the DITMAC spanning across Counterintelligence (CI), Behavioral Analysis, Law Enforcement (LE), Personnel Security, and Industrial Security. We provide internal training on the DITMAC System of Systems (DSoS) and a DITMAC 101 for all analysts. We also host regular 'lunch and learn' sessions for DITMAC employees where we bring in briefers on a variety of topics to foster a culture of continual learning.

Component #1

- Our InT Training Plan mostly leverages training outside, but within the Federal govt, mostly DoD (CDSE, DIA, etc.) and the National Insider Threat Task Force (NITTF).
    - Note: Our component provides supplemental privacy and civil liberties training for Hub personnel
- Our InT Training Plan is currently tailored for four audience categories: general workforce, senior official/program manager, program management personnel, and operational staff. In the long term, audience categories will expand to specific roles such as Hub Analyst. The curriculum will most likely include the CDSE Hub related courses (ETA FY18-20). In the meantime, the Hub Analyst curriculum is covered in the following categories:
    - Our InTP management personnel are those with the responsibility for establishing, supervising, and/or managing Hub-level operations within the InTP
    - Our InTP operational staff are personnel with responsibilities in participating in Hub-level operations
- Program management and operational staff should complete the applicable activities from our InT Training Plan in order to perform their assigned InT duties. Note: specific job functions may require additional training such as for the DSoS.

- General InT Program Management
    - It is recommended that program management personnel take the NITTF Hub Operations course and/or the Software Engineering Institute/Carnegie Mellon University Insider Threat Program Manager: Implementation and Operation course
- CI and Security Fundamentals
- Legal issues
    - Laws and regulations regarding data protection, collection, safeguarding, retention and lawful use of data and records
    - Privacy and civil liberty laws
        - Our component provides supplemental training to Hub analysts and other operational and program personnel where there are gaps identified in current DoD level training.
    - Response actions
    - LE investigation referral requirements in accordance with Section 811 of the Intelligence Authorization Act for FY 1995. Our components special investigations personnel assigned to an InTP function need the 811 training; others should have a general understanding of the process and reporting requirements.
- DSoS account training prerequisites (only for those who need access to the system)
    - IAA Cyber Awareness Challenge
    - Intelligence Oversight Course
    - Identifying and Safeguarding Personally Identifiable Information (PII)

Component #2

As for formal in-person training, Hub personnel are required to attend the NITTF Hub Operations Course. However, per Hub Standard Operating Procedure (SOP) guidance, Hub personnel are also required to complete the following internal training requirements. There are no “analysts” currently assigned as personnel performing Hub operations are not full time.

- Insider Threat Program Overview (Annually)
- Insider Threat Response Actions (Annually)
- CI Functional Training (One-Time)
- Section 811 Referral training (Annually)
- Information Security Refresher Training (Annually)
- Privacy and Civil Liberties Refresher Training (Annually)
- Counterintelligence Awareness Training (Annually)

Component #3

We do not offer any type of analysis or analytical training for the InTP analyst. We are budgeted for one analyst and one Program Manager (PM). We are researching course availability, pricing and opportunities that would enable us to improve our analysis skills. Our Hub members are required to attend the NITTF Insider Threat Hub Operations course, as well as PII, Civil Liberties, Privacy Act, Counter Intelligence, and OPSEC training.

Component #4

We use CDSE and have members of the DITMAC conduct demos.
We're planning to visit the DITMAC in the future.
Our primary members will be attending the NITTF Hub course (2/4 completed to date).

Component #5

Other than legal, privacy and civil liberties training, all Hub analysts are trained externally. The training consists of Splunk (basic and advanced), Lexis Nexus, 811 Referral, and Computer Network Log Analysis.

All Hub personnel have a background as an all-source, CI, or LE analyst.

Q2. Is there a specific set of performance, curriculum, or training requirements that your Hub analysts must meet, or skills they must possess? If so, can you explain? Could you share this with other PM's?

DITMAC

The DITMAC established a core set of skills desired while conducting the hiring process for InT analysts. In addition, the DITMAC established a training curriculum that highlights required training as well as supplementary training that can be taken to promote continual learning amongst our analysts. The DITMAC identified several baseline courses that every analyst must attend or have previously attended regardless of grade level. The courses identified assist the InT analyst with acquiring baseline training in Analysis, CI, LE, Cyber, Security, and Human Resources. Once those courses are completed we have identified supplemental training that can be taken to further develop their skills and expertise.

Component #1

Hub analysts should be composed of wide ranging and varying skill sets across the CI, LE, physical/information security, and intelligence disciplines. You want your InT indicators to be looked at from all discipline "lenses" to ensure you have the correct context. The synergy between analysts of varying expertise has proven very successful in our existing program.

Component #2

See previous question response

Component #3

Based on the current position description, our analyst fills a 0080 Security Specialist position and is required to complete the Security Fundamentals Professional Certification.

Component #4

Not established yet; drafting a PD for an analysis.
This will be an unfunded requirement for now.

Component #5

We have yet to formally establish official training requirements. However, all Hub personnel have a background as an all-source, CI, or LE analyst.

Q3. When training, are your analysts cross trained in multiple security fields and/or disciplines, or are they a Subject Matter Expert (SME) in a specific area?

DITMAC

Our analysts may come to the DITMAC with specific areas of expertise but the DITMAC ensures all InT analysts are cross trained in the multiple InT disciplines. DITMAC focuses on first training them to be analysts and then training the analysts to be conversant across CI, LE, Cyber, HR, and Security issues as they pertain to InT.

Component #1

We currently do not have a formal training program for our existing analysts. The training is OJT utilizing our UAM capability as well as hands on training from the UAM vendor.

The program is currently manned primarily by contract analysts. As part of the Statement of Work (SOW), we have identified that the analysts should have a wide ranging background and experience across multiple security fields. This has worked well for us as our analysts have expertise in CI, LE, Physical and Information Security, and Intelligence

Component #2

Personnel performing Hub operations are SMEs in specific fields (i.e. Personnel Security, Information, Security, Physical Security, CI, Legal, Privacy, Cyber, Investigations, etc.) The Assigned Insider Threat Program Manager has varied professional background in Security, CI, LE, Investigations (both Administrative and Criminal), etc.

Component #3

Our analysts are cross trained in multiple security areas to ensure they have at least a basic understanding of multiple security disciplines. We look for opportunities within our organization to provide training and education in areas outside of the InTP.

Component #4

Analysts will be cross-trained (Security, Cyber Security, HR, CIO, etc.)

Component #5

All analysts receive the same level of training. However, through the training process we have identified individuals that excel in analyzing specific data sets.

Q4. Do you envision that Hub analysts need to know the policy and directives associated with their responsibilities?

DITMAC

Yes, we believe this is a critical foundation for the analysts. The DITMAC developed an Analyst Reference Guide which includes such things as relevant National and DoD InT related policies, the Systems of Records Notice (SORN) and DITMAC thresholds to ensure all personnel are well versed in DITMAC and the DoD Component program's authority to conduct their mission.

Component #1

Yes! Absolutely

Component #2

Those associated with a viable InTP should be cognizant of federal laws, statutes, authorities, policies, programs, and resources in order to counter the InT. Additionally, these personnel must be SMEs so as to effectively advise Hub members in on-going activities.

Component #3

Hub analysts should know and understand National level guidance, DoD level guidance as well as their own component/agency guidance. Our analysts are involved in the development of agency level InT policies, directives, and instructions.

Component #4

It should be included in their PD.

Component #5

Yes, analysts benefit from an understanding of the policies and directives that empower their duties.

Q5. Does your InTP require or recommend professional certification(s) in the Hub? If so, can you specify?

DITMAC

At this time, the DITMAC does not require InT analysts to acquire or maintain professional certifications.

Component #1

We currently require all of our analysts to be at least 8570 IAT level 2 certified. The program coordinator PD has a requirement to hold 8570 IAM level 3 certification. Recommend certifications in information security as well as any relevant CI or physical security. But you may want to have SME’s with certain differing certs as opposed to everyone having the same certs.

Component #2

Not at this time. However, certifications will be considered as the InTP evolves.

Component #3

Our analyst position is a 0080 Security Specialist and is required to complete the Security Fundamentals Professional Certification via Defense Security Service.

Component #4

No, and it is unlikely now due to budget constraints.

Component #5

No, however our PM is certified by Carnegie Mellon (SEI) as a PM and an InT Vulnerability Assessor.

Q6. Outside of your own organizational training -- what Government sources or entities provide InT Hub training for your analysts? If so, what courses/focus?

DITMAC

In addition to internal DITMAC focused training, we leverage several courses offered by CDSE, USG providers (DNI, DIA) and commercial providers. These courses focus on Analysis, Critical Thinking, Briefing, CI, LE, Security, HR, and Cyber. In addition to the NITTF Hub Operations Course, some of these courses include the following:

> Classroom Course: DNI Analysis 101 (DIA-013598): ODNI's entry level course prepares new analyst to play their role in achieving the DNI's goal of transforming intelligence analysis and fully integrating the intelligence community (IC). The course brings together new analysts from throughout the IC during their initial months of the job for 2 weeks of rigorous training in a truly joint environment, equipping them with the basic critical thinking and analytic skills necessary to achieve the IC's published Analytic Standards.
>
> Classroom Course: Intelligence Analysis Course (DIA-005181): Trains newly-assigned intelligence personnel in the fundamentals of general intelligence analysis as preparation for assigned analytical duties. To educate the learner in critical thinking and the use of structured analytic techniques in order to mitigate biases and mindsets so as to produce the best possible analyses and assessments.
>
> Classroom Course: Critical Thinking and Structured Analysis (CTSA) (DIA-50604): Recognize biases, mindsets, mental shortcuts, and the problems they present for analyst; Apply critical thinking skills to mitigate biases, mindsets, and mental shortcuts; Use structured analysis techniques to study problems separately, systematically, and sufficiently. Distinguish between the concepts of critical thinking; identify the impact of cognitive bias on reasoning; and recognize the value of critical thinking.
>
> Classroom Course: Advanced Analytical Briefing Workshop (DIA-008236) (AGILE/NIPR): This course is open to DIA & non-DIA ICAAP participants and others looking to improve their briefing skills. The course is targeted toward GG-11 to GG-13, or higher personnel who have comparable briefing responsibilities. A total of three briefings are conducted, each in a different real world setting. Students will be required to have a briefing they are comfortable delivering in a maximum 10 minute time frame. (3 day course offered at DIA HQs).

Web-based Course: Analysis of Competing Hypotheses (JCA-ACH1) (AGILE/SIPR): This online course is designed to help the students understand the Analysis of Competing Hypotheses (ACH) tool, why it is used and how to apply ACH to counterintelligence and counterterrorism cases.

Classroom Course: Counterintelligence Analytic Methods (DIA-005207): Course provides a foundation for CI and intelligence analysts who work strategic and operational level all source counterintelligence analytic issues

Classroom Course: Federal Employee Relations (LABR 7009D): Understand the complexities of federal employee relations. Learn the rights and responsibilities of agency employees in areas such as probationary periods, performance management and awards, discipline, conduct problems, leaves of absence, labor management issues, appeals and grievances. This course is offered at USA Graduate School. There are costs associated with this course.

Web-based Course: (U) Investigative Planning (JCA-IP1) (AGILE/SIPR): This online course provides personnel with basic concepts of investigative planning. Upon completion of this training, students will be able to recognize the criminal elements of national security crimes and identify the key concepts of the investigative planning process

Web-based Course: Introduction to Personnel Security Source (DSS/CDSE): This course introduces the management practices and procedures required to administer the Department of Defense (DoD) Personnel Security Program (PSP) at the military base/installation level. The course provides an overview of the elements of the PSP to include: designation of sensitive duties; investigative and adjudicative practices; security officer responsibilities under the PSP one-time access requirements; special security program requirements; and due process procedures.

Web-based Course: Introduction to DoD Personnel Security Adjudications Course (DSS/CDSE): Learn what a security clearance, eligibility, and access are and how they related to classified information and the Personnel Security Program (PSP). How a favorable determination is made and it’s specific relationship to levels of access to classified information and assignment to sensitive positions.

Component #1

List of courses is included in our InT Training Plan; additional list in Appendix B; resources for learning activities listed in Appendix C. Examples: NITTF Hub Operations Course, DCITA Cyber Insider Threat Analysis, CERT SEI Insider Threat Program Manager

Component #2

NITTF – Hub Operations Course.

Component #3

We utilize the NITTF for the Hub Operations Course, and the FBI for 811 referral training.

Component #4

NITTF Hub Course.
Computer based training provided by CDSE.

Component #5

The NITTF Hub Course

Q7. Does your Hub use analysis training from commercial sources? If so, can you specify?

DITMAC

Yes, the DITMAC has identified a variety of commercial training courses that we include in our curriculum. We try to maximize the use of no-cost training but will leverage commercial training where gaps exist. For example, the USA Graduate School, Alpha Group, as well as CERT, provides training in some key areas.

Component #1

We use specialized training from our UAM vendor as one of our contract deliverables. This focuses on analysis within the tool as well as developing InT indicator “trigger” sets.

Component #2

Not at this time.

Component #3

We utilize our UAM contractor for software and user operations training.

Component #4

We will in the future, if we get funding for UAM.

Component #5

Splunk (Basic and Advanced)
Lexis Nexus

Q8. Are your InT analysts trained to the same level? Is the training based upon skill or experience?

DITMAC

Although, all analysts come to the DITMAC at varying levels of skills and experience, the DITMAC training plan ensures that all InT analysts meet the same initial baseline training requirements.

Component #1

Skill and experience, we have common vendor provided training to all analysts but our organization has junior and senior analysts based upon experience and skill level.

Component #2

N/A

Component #3

We are budgeted for one fulltime analyst and receive part-time support from the Force Protection Analyst. Both receive the same training to ensure we have backup capability in the program.

Component #4

No analysts are on board yet as this is an unfunded requirement.

Component #5

All analysts receive the same level of training.

Q9. Has NITTF established a standardized curriculum that is required for InT analysts?

NITTF

NITTF has not established a standard Executive Branch training curriculum plan in order to give departments and agencies more flexibility in satisfying the training elements outlined in White House Memo: National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, dated November 21, 2012.

Q10. How is training for Insider Threat Hub analysts different than general workforce training?

OUSD (I) & CDSE

Workforce training aims to provide awareness of the InTP and emphasize the importance of vigilance while maximizing trust and reporting. We are working to develop training that will be available to personnel directly supporting analytic hubs. It will entail specialized and tailored material that coincides with the associated duties and responsibilities of InT personnel. This training will initially look at fundamentals that all Insider Threat operations personnel should have and evolve into more robust courseware development at the intermediate and advanced level. CDSE provides training specialized for Insider Threat operations personnel and it includes: counterintelligence and security fundamentals, legal issues, laws and regulations regarding data protection, collection, safeguarding, retention, lawful use of data and records, privacy and civil liberty laws, response actions, law enforcement investigation referral requirements, and etc.

Q11. Can you describe the training you provide to the analyst?

CDSE

We do not specifically provide training to the analyst, but rather to InTP operations personnel who may consist of analysts and other security professionals.

The training specifically designed for the group is the following:

Current:
Establishing an Insider Threat Program for your Organization course
Insider Threat Job Aid for Industry Insider Threat Programs course
Sample Insider Threat Program Plan for Industry course
Insider Threat Training Requirements and Resources for DoD course
Continuous Monitoring Course
Insider Threat Case Study Series
Understanding Espionage and National Security Crimes Job Aid
DITMAC Short
Insider Threat Toolkit and Vigilance Campaign
Webinars: Insider Threat with OUSDI, Insider Threat with DITMAC, Cyber Insider Threat, Behavioral Analysis in Insider Threat, PEI: Detecting Actions outside the norm, Adverse information reporting, Virtual Insider Threat Symposium for Industry

In Development FY17:
Insider Threat Indicators in Records Checks course
Insider Threat Mitigation Response Options course
Building Multidisciplinary Insider Threat Capability course
Preserving Investigative and Operational Viability in Insider Threat course
Insider Threat Requirements for Senior Leadership short
Insider Threat Indicators in User Activity Monitoring webinar/job aid
Additional Insider Threat Case studies and vigilance campaign materials

Future Intentions:
DoD Insider Threat Program Hub Course
Privacy and Civil Liberties for DoD Insider Threat Programs course
Critical Thinking for DoD Insider Threat Programs course

NITTF

The NITTF only offers the Hub Operations course.

This course introduces and exercises the basic functions of an InTP's centrally managed analysis and response capability (referred to as the "Hub"), to gather, integrate, analyze, and respond to potential InT information derived from CI, security, information assurance, HR, LE, and other internal and external sources. This is a practical, scenario-based course designed to expose InT personnel to realistic events in the day-to-day operations of an InT Hub. The class will include break-out sessions with an assigned instructor/facilitator for specialized attention. The Topics include:

- Insider Threat Program principles and functions
- Legal underpinnings and considerations
- Operational fundamentals and processes
- Response and referral actions
- Reporting and documentation concepts

The course length is 3 days (0800 – 16:00), Tuesday – Thursday.

Beginning March 13th, NITTF will no longer use AGILE for Hub Course registration processing. DoD Insider Threat Program Managers or designated officials can submit requests for their Insider Threat personnel direct to NITTF via either of two email organizational accounts: NITTF_Training@dni.gov or NITTF-Assistance@dni.gov. Requests must include name, organization, duty title, unclassified email address, and employment status (government or contractor). If contractor, include a statement that your agency COTR approves of the individual receiving this government training.

Q12. Where is DoD with certification programs for InT analysts?

OUSD (I)

Although DoD does not currently have certification programs for Insider Threat personnel, professionalizing the Insider Threat workforce through certification is a long term goal for the Department. OUSD (I) is currently exploring optimal courses of action and is working collaboratively with CDSE, NITTF and other stakeholders across the community. OUSD (I) is also working to have Insider Threat and the Countering Insider Threat mission included in other certification programs. Insider Threat is projected to be included in the Intelligence Fundamentals Professional Certification Program as a topic area. This certification program is being developed at the unclassified level. More details to follow as this program comes online.

Q13. Where can Components find the training curriculums and other key information pertaining to analysis training aforementioned in this document?

OUSD (I)

There are some excellent training programs developed Components. If you are interested in any of the training curriculums/standardized trainings or other key information pertaining to analysis training in this Best Practices edition, please contact the DoD Insider Threat Program and we will provide you contact info. Participating Components have stated that they are willing to share their specific programs/information to those InTPs that reach out directly.

Attachment 1

CDSE Insider Threat Training Requirements and Resources

Attachment(s) are on the following pages

Center for Development of Security Excellence

CDSE

Learn. Perform. Protect.

INSIDER THREAT

JOB AID

Insider Threat Program Management Personnel Training Requirements and Resources for DoD Components

National Minimum Standards require Insider Threat Program Management personnel receive training in:

- Counterintelligence and Security Fundamentals
- Laws and Regulations about the gathering, retention, and use of records and data and their misuse
- Civil Liberties and Privacy Laws, Regulations, and Policies
- Referral processes, regulations, and requirements including Section 811 of the Intelligence Authorization Act
- Internal agency procedures for insider threat response actions

The following training resources—including general training and additional beneficial training—have been identified but are not necessarily endorsed. Industry partners under the NISP click **here**.

General Insider Threat Program Personnel Training

CDSE eLearning: Establishing an Insider Threat Program for Your Organization CI122.16

NITTF Instructor Led: Insider Threat Hub Operations Course

*Both courses require supplemental, DoD specific privacy, civil liberty, intelligence oversight, and referral training.

CI and Security Fundamentals

CDSE eLearning Courses

- Insider Threat Awareness Course CI121.16 (also available on AGILE high side)
- Introduction to Personnel Security PS113.16
- Personnel Security Management PS212.01
- Developing a Security Education and Training Program GS104.16
- Introduction to DoD Security Specialist Course GS020.16
- Counterintelligence Awareness and Reporting Course for DoD Employees CI116.06
- Counterintelligence Awareness and Security Brief CI112.16
- Counterintelligence Concerns for National Security Adjudicators CI020.16

CDSE Instructor-led Courses

DoD Security Specialist GS101.01

DIA eLearning: Counterintelligence Awareness and Reporting (on AGILE)

Joint Counterintelligence Training Academy (SIPR https://jcitajvta.dia.smil.mil/)

- Counterintelligence Fundamentals web based training
- Defense Counterintelligence Agent Credentialing Course

Laws and Regulations about the gathering, retention, and use of records and data and their misuse/ Civil Liberties and Privacy Laws, Regulations, and Policies

CDSE eLearning: Identifying and Safeguarding Personally Identifiable Information (PII) DS-IF101.06

Joint Knowledge Online (accessible with CAC) various offerings in Privacy Act Awareness, Protecting PII, and Intelligence Oversight.

Defense Privacy and Civil Liberties Division privacy and civil liberties training, civil liberties instruction

Department of Justice, Office of Privacy and Civil Liberties (OPCL) provides privacy training through the Executive Office for United States Attorneys, Office of Legal Education. Including online FOIA training.

Icompass (WHS) OSD/Joint Staff Privacy Act training

eLearning available on AGILE:

NGA Intelligence Oversight Training
NGA Privacy Awareness
Intelligence Oversight Officer/Supervisor Course – OSD
Intelligence Oversight Training Course "IO-101" – OSD
Introduction to Intelligence Oversight - DIA

Referral Processes and Reporting Requirements to include Section 811 Referrals*

CDSE eLearning Courses

- JPAS/JCAVS Virtual Training for Security Professionals PS123.16
- Reciprocity in the Personnel Security Program *Learning Short
- Adverse Information Reporting *Learning Short

Federal Bureau of Investigation

- 811 Referral Training is provided by the FBI in the Washington Metropolitan area on an annual basis. POC: Steve Jarnecki, 202-324-7689

- 811 Referrals may be sent directly to the FBI:

  For Secret referrals: HQ_DIV05_CD_FBI811SECRET@fbi.sgov.gov

  For TS referrals: HQ_DIV05_CD_FBI811TOPSECRET@fbi.ic.gov

  Questions should be referred to CD4 Assistant Section Chief Michael Varacalli, Desk: 202-324-4556, UNET: ormichael.varacalli@ic.fbi.gov or Assistant General Counsel Mitchell B. Weiss, Desk: 202-324-1959

*For cleared industry, these referrals are equivalent to those under section 1-301 of the National Industrial Security Operating Manual.

Agency Procedure for Insider Threat Response Actions

Agency or component dependent.

Additional Training beneficial to Insider Threat Program Management Personnel

- User Activity Monitoring Training: vendor specific
- Cybersecurity
    - Defense Cyber Training Academy—Online, Instructor Led, and Blended:
    - DCITA: Cyber Insider Threat Analysis Course
    - DCITA: Introduction to Cyber Insider Threat
    - DCITA: Network Monitoring Course
- Videos: DNI/NCSC Video Series: Terminal Risk

CDSE Instructor-led Courses

- Information Security Management IF201.01
- DoD Security Specialist GS101.01
- Personnel Security Management PS212.01
- ODNI/ONCIX ICD 704 Personnel Security Course FT106.01

CDSE eLearning Courses

- Introduction to Information Security IF011.16
- Introduction to Risk Management GS150.06
- Risk Management for DoD Security Programs GS102.16
- Unauthorized Disclosure of Classified Information for DoD and Industry IF130.16
- Introduction to DoD Personnel Security Adjudication PS001.18
- Introduction to National Security Adjudications PS170.16
- Introduction to Personnel Security PS113.16
- Introduction to Suitability Adjudications for the DoD PS010.16
- Continuous Monitoring CS200.16
- Cyber Insider Threat *Webinar
- Active Shooter Awareness *Learning Short
- Insider Threat for DoD Security *Webinar
- Potential Espionage Indicators (PEI): Detecting Actions Outside the Norm *Webinar

CDSE Job Aids

Insider Threat Case Studies
Understanding Espionage and National Security Crimes

Toolkits

- Counterintelligence Awareness
- Insider Threat
- Adjudicators
- Personnel Security

Coming Soon from CDSE: DITMAC Short eLearning