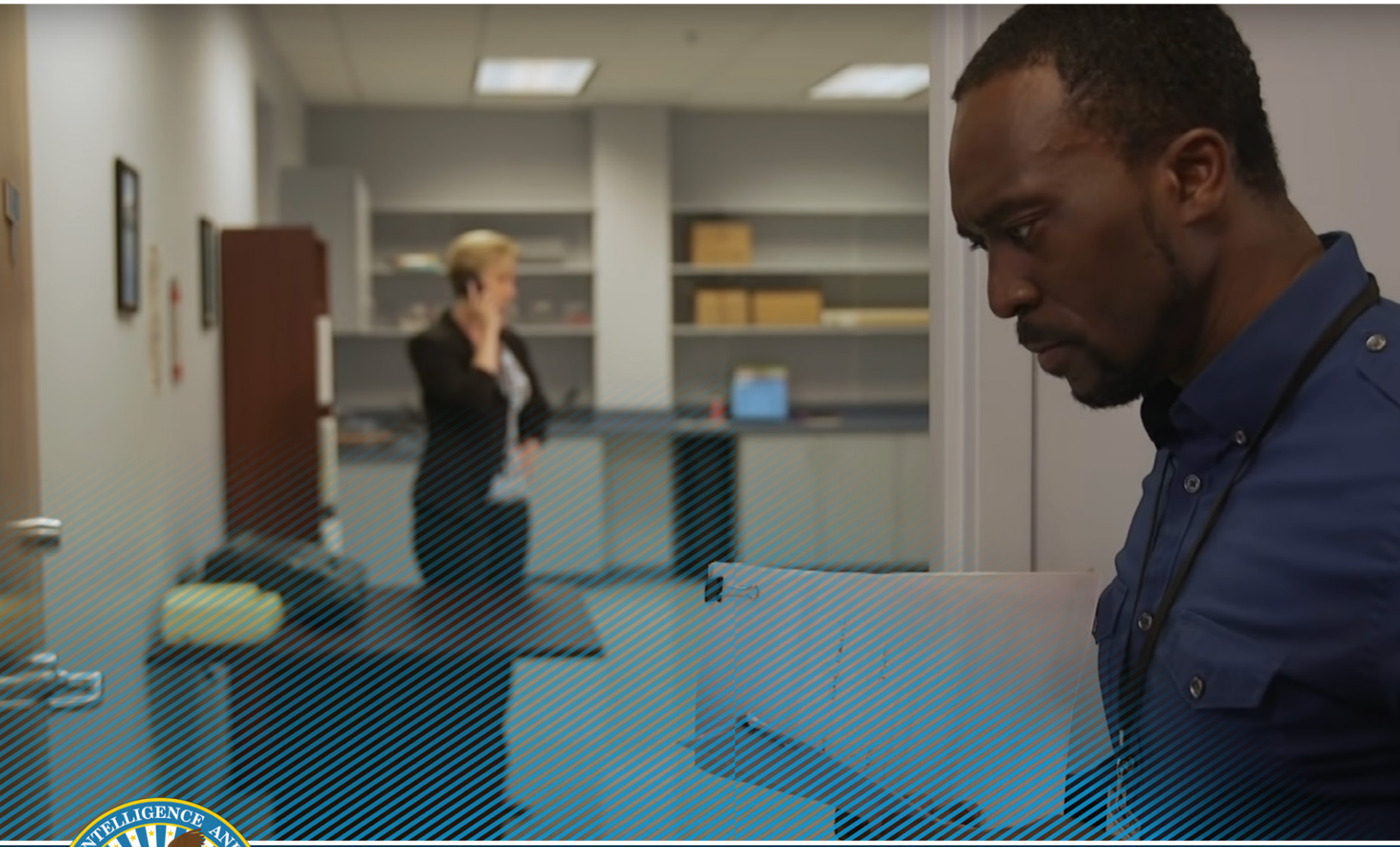
CDSE INSIDER THREAT VIGILANCE VIDEO SERIES

SEASON 1: TURNING PEOPLE AROUND, NOT TURNING THEM IN

FACILITATION GUIDE



CDSE Center for Development of Security Excellence

www.cdse.edu

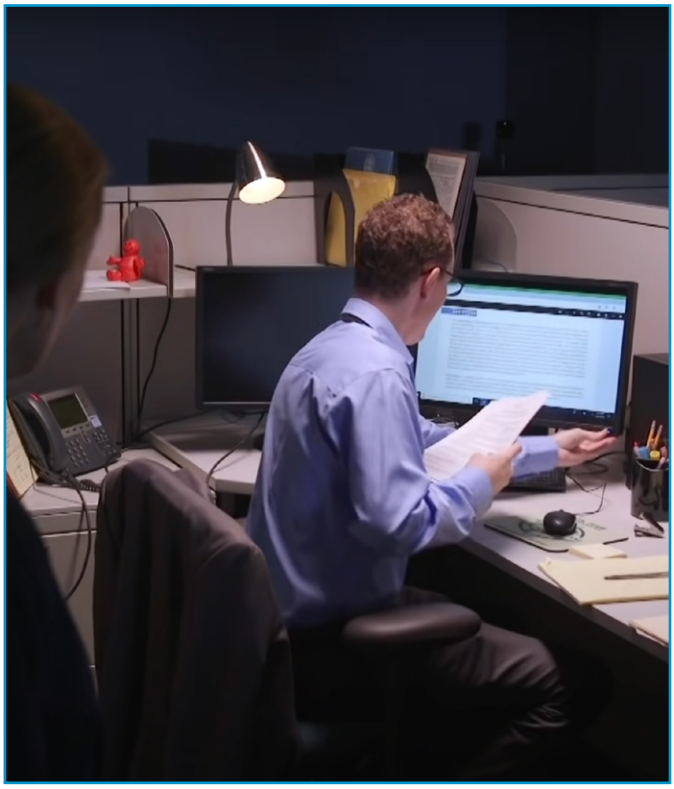
SEASON OVERVIEW

In Season 1 of the "CDSE Insider Threat Vigilance" series, Tim and Phyllis begin displaying some behaviors that come to the light of their coworkers, enough so that one of them reports it to the insider threat team, which conducts inquiries and convenes to discuss their findings. Season 1 illustrates the effectiveness of a multi-disciplinary insider threat program approach towards analyzing information and activity indicative of an insider threat. The goal is to deter threats and detect potential issues early on – before a problem occurs. In a final twist, we see that those who may have been viewed as the potential insider threats really were not, and that insider threats can be the results of the actions of the unwitting.

TAKEAWAYS

- Insider threats can be witting and unwitting. Failure to follow procedures or policies may result in an insider threat incident.
- Insider threat programs are most effective when they utilize a multi-disciplinary approach involving all the insider threat pillars.
- Insider threat programs must conduct and analyze all the information in an unbiased manner to fully understand whether or not the reported behaviors and actions warrant further investigation or referral.
- Recognizing and reporting potential risk indicators of insider threat enables early intervention and timely support, leading to positive outcomes for the individual, the organization, and the mission.
- Engagement by those who are closest to the individual, such as coworkers and management, may provide much-needed information and clarification concerning an individual's behavior and actions.

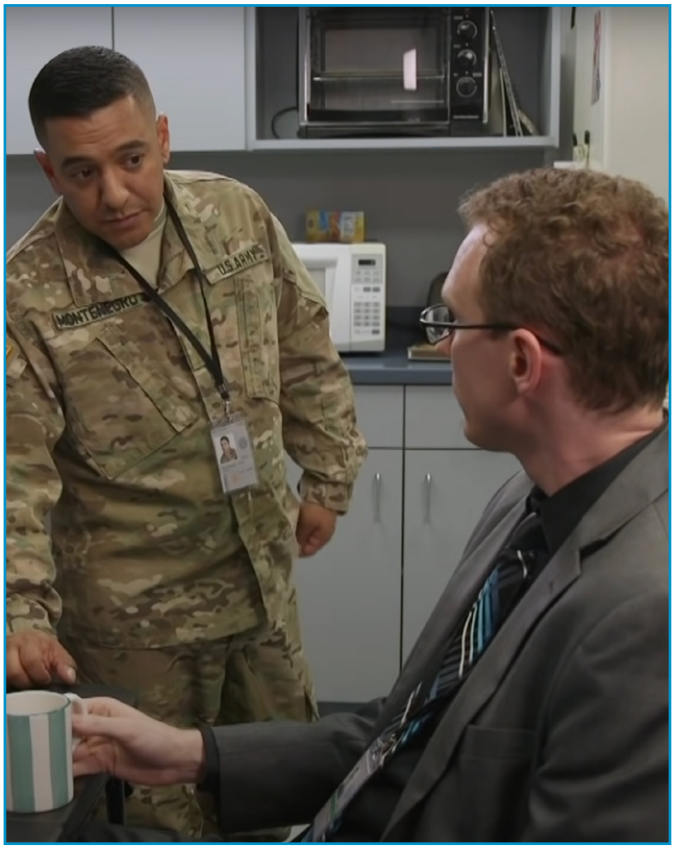
Episode 1: "An Odd Encounter with Tim"



Tim's co-workers begin noticing what they perceive to be odd behaviors. One of his co-workers reported the behavior to the insider threat team and another did not. Episode 1 focuses on identification and reporting of such odd behaviors which may be potential risk indicators.

- Why was Tim's talking low on his phone, working alone late, quickly minimizing his computer screen and shutting it down, and rushing off leaving his food and beverage on his desk considered odd behavior by Susan?
- Susan considered Tim's behavior odd and potential risk indicators. What should she do?
- Why did Beth not take immediate adverse actions against Tim? What are the next steps for Beth?
- What makes up an effective multi-disciplinary insider threat team? What areas of expertise are present in the team in the video?

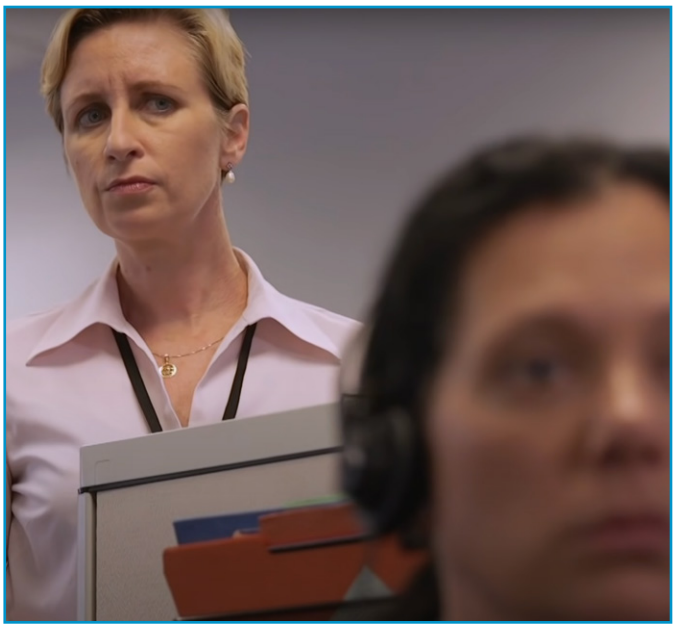
Episode 2: "Check Out My New Ride"



After conversing with Tim, his co-worker, Major Montenegro finds some of what Tim says to be odd and perhaps something he should address further such as Tim recently suddenly purchasing a new car, calling off his engagement and splitting up with his girlfriend, and putting in a two-week notice. Tim's behavior catches the attention of another of his coworkers. Episode 2 expands on the topic of identification and reporting.

- Why were Tim's behaviors considered to be potential risk indicators by Major Montenegro?
- Should Major Montenegro report what he learned from speaking with Tim or should he keep it confidential because it was a private conversation?
- Taking into account what is learned about Tim, when does a behavior or action reach the threshold for reporting?
- Where can Major Montenegro go to discuss his suspicions about Tim?

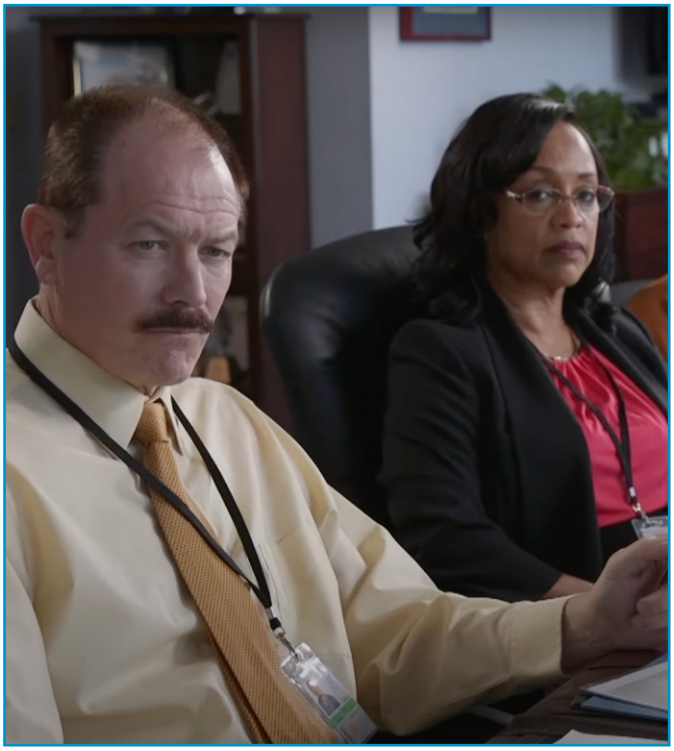
Episode 3: "What's Pre-Publication Review?"



After learning about some odd behavior from Tim, we then learn that another co-worker is displaying some odd behavior. Episode 3 focuses on this individual and how their actions can potentially make someone an unwitting insider threat.

- What behaviors did Phyllis display that made Stuart suspicious?
- Why could Phyllis's behavior be considered potential risk indicators?
- Why is pre-publication review important?
- What could happen if an individual releases an organization's Information before it is reviewed and approved?

Episode 4: "Meeting of the Minds"



After receiving reports from Tim's co-workers, the insider threat team convenes but then directs its focus on the actions of one of his co-workers. Episode 4 focuses on the insider threat team and its multi-disciplinary approach to responding to insider threat reporting.

- After directing its attention to one of Tim's co-workers, what was the assessment by the insider threat team regarding Tim and his behavior?
- In this episode, what components of a multi-disciplinary insider threat team were present?
- Where might the agency have to report Joyce's unauthorized disclosure and what role do they play?
- How can the unwitting actions of an individual lead to an insider threat incident?

POLICIES AND GUIDELINES

The Department of Defense Insider Threat Program – DoD Directive 5205.16

Season 1 addresses identification of potential risk indicators and reporting as well as the components of a multi-disciplinary insider threat program. DoD 5205.16 establishes policy and assigns responsibilities within DoD to develop and maintain and insider threat program to comply with the requirements and minimum standards to prevent, deter, detect, and mitigate the threat insiders may pose to DoD and U.S. Government installations, facilities, personnel, missions, or resources. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or the loss or degradation of departmental resources or capabilities. It ensures appropriate DoD policies, including but not limited to counterintelligence (CI), cybersecurity, security, civilian and military personnel management, workplace violence, emergency management, law enforcement (LE), and antiterrorism (AT) risk management, are evaluated and modified to effectively address insider threats to DoD.

To learn more, read the full **DOD Directive 5205.16**.

Security Executive Agent Directives (SEAD)

The SEAD establishes the policies and procedures governing investigations and adjudications for eligibility for access to classified information or eligibility to hold a sensitive position.

- **SEAD-3** establishes reporting requirements for all covered individuals who have access to classified information or hold a sensitive position.
- **SEAD-4** establishes the adjudicative guidelines for all covered individuals who require initial or continued eligibility for access to classified information or eligibility to hold a sensitive position.
- **SEAD-5** establishes guidelines for the collection, use, and retention of social media information.
- **SEAD-6** establishes policies and requirements for the continuous evaluation of covered individuals.

Review all the directives on the **Director of National Intelligence website.**

ADDITIONAL RESOURCES

Supporting Through Reporting

Recognizing and reporting potential risk indicators enables early intervention and timely support, leading to positive outcomes for the individual, organization, and the mission. For individuals who require national security eligibility for sensitive positions or access to classified information, certain reporting requirements are mandatory.

To learn more, see the CDSE's **Insider Threat Potential Risk Indicators Job Aid**.

Unauthorized Disclosure

Cleared individuals have an obligation to protect classified information. Failure to do so can result in damage to national security and the warfighter. There are approved channels to report fraud, waste or other abuse through existing whistleblower or Inspector General channels. There are also approved channels for the release and review of DoD information.

The CDSE's **Unauthorized Disclosure Toolkit** will help you learn the difference, where and how to report both unauthorized disclosure, questionable government behavior and activities, and more. Unauthorized disclosure is not whistleblowing; it's a crime.

NOTE: If the URLs in this document do not open upon clicking, right-click on the hyperlinked text, copy link location, and paste into a browser. Alternatively, you can open the PDF in a browser.