



Center for Development  
of Security Excellence  
**CDSE**

## INSIDER THREAT JOB AID



### FACILITATION GUIDE

#### **Insider Threat Vigilance Video Series – The Critical Pathway: Episode One, “Organizational Trust”**

**Overview:** The Insider Threat Vigilance Series aids the workforce in understanding how to identify and report insider threat indicators. The series also provides an overview of how Insider Threat Programs take a multi-disciplinary approach towards analyzing information and activity indicative of an insider threat and referring pertinent data to the appropriate officials for investigation and resolution. The goal of the program is to deter threats and detect potential issues before a problem occurs.

This guide will aid in presenting the video to the training audience. Use the questions below to assist with a group discussion. You can access the episode on YouTube or in a micro-learning module with expanded information and resources.

**YouTube Location:** <https://www.youtube.com/watch?v=TLmtdu8ZICk>

**Micro-Learn Location:** <https://www.cdse.edu/micro/critical-episode1/critical-episode1.html>

---

#### **Instructions**

**Video Segment 1: Play the video. Then pause at 02:41 and consider asking students the following question.**

**How might budget cuts influence the threat environment for this organization and others?**

**Desired responses:**

- Increased potential for insider threat activity or espionage
- Increased potential for employee disgruntlement

**Video Segment 2: Un-pause the video, and pause again at 06:02. Consider asking students the following questions.**

**What organizational changes, if any, have occurred or may soon occur?**

**Desired responses:**

- No additional bonuses or approval for overtime
- No contract renewal for federal contractors
- Loss of employment
- Increased workload for federal workers

## How might this organizational change affect Rachel or Antonio?

### Desired responses:

- Antonio may face increased stress over paying bills (new mortgage); financial concern
- Rachel may not be able to go on vacation; financial concern

## Video Segment 3: Un-pause the video and play it through to the end. Consider asking the following questions.

## Why is organizational trust important during change?

### Desired responses:

- Potential for increased job satisfaction
- Potential for increased morale
- Potential for increased participation in programs (EAP and Insider Threat)

## How did leadership seek to maintain trust during this time of organizational change?

### Desired responses:

- Organized mandatory briefings to maintain transparency about the effects of budget cuts
- Made plans to ask human resources to reach out to every employee
- Reminded employees that Employee Assistance Programs are an additional source of support

**Possible Discussion:** Are there other ways leadership could have improved organizational trust? Please take the opportunity to discuss trust within your own organization.

---

## Additional Facilitator Resources

**Insider Threat Toolkit:** <https://www.cdse.edu/toolkits/insider/index.php>

**Insider Threat Vigilance Video Series – Turning People Around, Not Turning Them In: Episode One, “An odd encounter with Tim”:** <https://www.cdse.edu/micro/vigilance-episode1/vigilance-episode1.html>

**Insider Threat Case Studies:** <https://www.cdse.edu/resources/case-studies/insider-threat.html>

# FACILITATION GUIDE

## **Insider Threat Vigilance Video Series – The Critical Pathway: Episode Two, “Indicators”**

**Overview:** The Insider Threat Vigilance Series aids the workforce in understanding how to identify and report insider threat indicators. The series also provides an overview of how Insider Threat Programs take a multi-disciplinary approach towards analyzing information and activity indicative of an insider threat and referring pertinent data to the appropriate officials for investigation and resolution. The goal of the program is to deter threats and detect potential issues before a problem occurs.

This guide will aid in presenting the video to the training audience. Use the questions below to assist with a group discussion. You can access the episode on YouTube or in a micro-learning module with expanded information and resources.

**YouTube Location:** <https://www.youtube.com/watch?v=MrsY64oTQr4>

**Micro-Learn Location:** <https://www.cdse.edu/micro/critical-episode2/critical-episode2.html>

---

### **Instructions**

**Video Segment 1: Play the video. Then pause at 04:30 and consider asking students the following question.**

**What are some of Rachel and Antonio’s personal predispositions and stressors?**

**Desired responses:**

- Rachel does not want to disappoint her husband
- Rachel’s real estate properties are not doing well
- Rachel’s property taxes are a concern
- Rachel had to sell her car dealership
- Antonio does not have any new employment prospects
- Antonio’s mortgage payment and student loan payments are a concern

**Video Segment 2: Un-pause the video, and pause again at 06:22. Consider asking students the following questions.**

**Were Antonio and Rachel’s social media problematic?**

**Desired responses:**

- Operational security concerns
- Oversharing of personally identifiable information
- Interaction with Brittany (coincidental)

**Is there any particular risk associated with Brittany’s solicitation over social media?**

**Desired responses:**

- Potential risk or increased susceptibility for targeting by foreign intelligence entities

**Who do you think is more likely to have accepted Brittany's offer?**

**Desired responses:**

- Both Antonio and Rachel have financial stressors
- There is not enough information available at this time to make that judgement

**Video Segment 3: Un-pause the video and play it through to the end. Consider asking the following questions.**

**What potential risk indicators did Rachel and Antonio exhibit?**

**Desired responses:**

- Rachel asked for information she did not have regular access to or the need-to-know
- Rachel worked overtime without permission
- Antonio's disgruntlement and outburst
- Antonio has not been attending meetings

**Possible Discussion:** Please take the opportunity to discuss other behaviors that may be considered potential risk indicators.

---

### **Additional Facilitator Resources**

**Insider Threat Toolkit:** <https://www.cdse.edu/toolkits/insider/index.php>

**Insider Threat Vigilance Video Series – Turning People Around, Not Turning Them In: Episode Two, “Check out My New Ride”:** <https://www.cdse.edu/micro/vigilance-episode2/vigilance-episode2.html>

**Insider Threat Case Studies:** <https://www.cdse.edu/resources/case-studies/insider-threat.html>

**Insider Threat Potential Risk Indicators Job Aid:** <https://www.cdse.edu/documents/toolkits-insider/INTJ0181-insider-threat-indicators-job-aid.pdf>

# FACILITATION GUIDE

## **Insider Threat Vigilance Video Series – The Critical Pathway: Episode Three, “See Something, Say Something”**

**Overview:** The Insider Threat Vigilance Series aids the workforce in understanding how to identify and report insider threat indicators. The series also provides an overview of how Insider Threat Programs take a multi-disciplinary approach towards analyzing information and activity indicative of an insider threat and referring pertinent data to the appropriate officials for investigation and resolution. The goal of the program is to deter threats and detect potential issues before a problem occurs.

This guide will aid in presenting the video to the training audience. Use the questions below to assist with a group discussion. You can access the episode on YouTube or in a micro-learning module with expanded information and resources.

**YouTube Location:** <https://www.youtube.com/watch?v=ydaQzdz2TG8>

**Micro-Learn Location:** <https://www.cdse.edu/micro/critical-episode3/critical-episode3.html>

---

### **Instructions**

**Video Segment 1: Play the video. Then pause at 03:52 and consider asking students the following questions.**

**What adverse information or potential risk indicators should be reported regarding Antonio and Rachel?**

**Desired responses:**

- Antonio’s work behavior and attendance have gone downhill
- Antonio’s admitted foreign contact
- Rachel’s sudden plan for foreign travel without a financial backing
- Rachel asking various coworkers for information without the need-to-know

**Where is potentially anomalous or risky behavior associated with an insider threat reported?**

**Desired responses:**

- Insider Threat Program
- Department of Defense: employees may consult their security officer or supervisor (if thresholds are met, reporting to Defense Insider Threat Management and Analysis Center of the Federal Bureau of Investigation may be required)
- Federal Agencies: employees may consult their security officer or supervisor (if thresholds are met, reporting to the Federal Bureau of Investigation may be required)
- Cleared Industry: Insider Threat Program senior official or facility security officer (if thresholds are met, reporting to the Federal Bureau of Investigation may be required)

**Video Segment 2: Un-pause the video, and pause again at 05:53. Consider asking students the following question.**

**How can leadership mitigate the risky behavior Antonio is exhibiting?**

**Desired responses:**

- Refer Antonio to the employee assistance program for counseling
- Give Antonio an insider threat awareness briefing

**Video Segment 3: Un-pause the video and play it through to the end. Consider asking the following questions.**

**Why might coworkers elect not to report information to a supervisor or Insider Threat program?**

**Desired responses:**

- They do not want to get anyone in trouble
- They do not trust the organization to handle the situation justly
- They are unaware of potential risk indicators and the threats an insider can pose to national security

**Possible Discussion:** What are the repercussions for the organization and the individual that elects not to report potential risk indicators?

---

### **Additional Facilitator Resources**

**Insider Threat Toolkit:** <https://www.cdse.edu/toolkits/insider/index.php>

**Insider Threat Vigilance Video Series – Turning People Around, Not Turning Them In: Episode Three, “What’s Pre-Publication Review?”:** <https://www.cdse.edu/micro/vigilance-episode3/vigilance-episode3.html>

**Insider Threat Case Studies:** <https://www.cdse.edu/resources/case-studies/insider-threat.html>

**Insider Threat Reporting Job Aid:** <https://www.cdse.edu/documents/toolkits-insider/INTJ0174-insider-threat-reporting-proc.pdf>

# FACILITATION GUIDE

## Insider Threat Vigilance Video Series – The Critical Pathway: Episode Four, “Outcomes”

**Overview:** The Insider Threat Vigilance Series aids the workforce in understanding how to identify and report insider threat indicators. The series also provides an overview of how Insider Threat Programs take a multi-disciplinary approach towards analyzing information and activity indicative of an insider threat and referring pertinent data to the appropriate officials for investigation and resolution. The goal of the program is to deter threats and detect potential issues before a problem occurs.

This guide will aid in presenting the video to the training audience. Use the questions below to assist with a group discussion. You can access the episode on YouTube or in a micro-learning module with expanded information and resources.

**YouTube Location:** <https://www.youtube.com/watch?v=ZQ-A5PzQvg8>

**Micro-Learn Location:** <https://www.cdse.edu/micro/critical-episode4/critical-episode4.html>

---

### Instructions

**Video Segment 1: Play the video. Then pause at 02:05 and consider asking students the following questions.**

**Which pillars of countering insider threat may aid the Insider Threat Program Manager in his risk assessment and mitigation of Rachel?**

**Desired responses:**

- Security (Physical, Personnel, Facility)
- Information Technology (Cybersecurity, User Activity Monitoring)
- Human Resources
- Law Enforcement
- Counterintelligence
- Legal Counsel

**Was the Insider Threat Program Manager correct to make an 811 referral to the Federal Bureau of Investigation? If so, why?**

**Desired responses:**

- Counterintelligence concerns
- Involvement of classified information
- Involvement of unauthorized disclosure
- Connection to foreign power or agent of foreign power
- Section 811 of the Intelligence Authorization Action of 1995 (50 US Code 402a) is the legislative act that governs the coordination of counterintelligence investigations between Executive Branch agencies and departments and the FBI. Section 811 referrals are reports that advise the FBI of any information, regardless of origin, that may indicate that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or agent of a foreign power.

**Video Segment 2: Un-pause the video, and pause again at 04:09. Consider asking students the following question.**

**Which insider derailed from the critical path of becoming an insider threat? And how?**

**Desired responses:**

- Antonio (found new employment)
- Antonio rejected online solicitation from Brittany (will be obvious if students have seen earlier episodes)
- Although he was disgruntled, Antonio still reported suspicious activity to the Insider Threat Program to prevent harm from occurring to the organization or national security

**Video Segment 3: Un-pause the video and play it through to the end. Consider asking the following questions.**

**What are the consequences Rachel and the other insider threats faced after being detected?**

**Desired responses:**

- Time in prison
- Fines
- Destruction of reputation and credibility
- Loss of employment

**Possible Discussion:** What is an Insider Threat Program? How can you report to an Insider Threat Program?

---

### **Additional Facilitator Resources**

**Insider Threat Toolkit:** <https://www.cdse.edu/toolkits/insider/index.php>

**Insider Threat Vigilance Video Series – Turning People Around, Not Turning Them In: Episode Four, “Meeting of the Minds”:** <https://www.cdse.edu/micro/vigilance-episode4/vigilance-episode4.html>

**Insider Threat Case Studies:** <https://www.cdse.edu/resources/case-studies/insider-threat.html>

**What’s the 411 on the 811 Job Aid:** <https://www.cdse.edu/documents/cdse/fbi-referral-job-aid.pdf>