



# Ensuring Fairness and Enhancing the Protection of Privacy in Counter-Insider Threat Programs

**Resources and Reflection Activities**

**October 2022**

**AUTHORS**

Lorien Megill, Jennifer VanBerschot,  
Kirk Kennedy, Zac Van Note, Callie Chandler, Andrée Rose

OPA Report No. 2022-177 | PERSEREC-PA-22-17



## Authors

### DEFENSE PERSONNEL AND SECURITY RESEARCH CENTER

Callie Chandler  
Andrée Rose

### PERATON

Kirk Kennedy

### NORTHROP GRUMMAN

Lorien Megill  
Jennifer VanBerschot  
Zac Van Note

## Sponsors

---



PERSEREC is a Department of Defense entity dedicated to improving the effectiveness, efficiency, and fairness of DoD personnel suitability, security, and reliability systems. PERSEREC is part of the Office of People Analytics (OPA), which is a component of the Defense Human Resources Activity (DHRA) under the Office of the Under Secretary of Defense (Personnel and Readiness).



Within the National Counterintelligence and Security Center (NCSC), the primary mission of the National Insider Threat Task Force (NITTF) is to develop a Government-wide insider threat program for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation.



The Office of the Secretary of Defense (OSD) is responsible for policy development, planning, resource management and program evaluation. OSD includes the offices of top civilian defense decision -makers with regard to personnel, weapons acquisition, research, intelligence and fiscal policy, as well as offices the Secretary establishes to assist in carrying out assigned responsibilities.

---

## Point of Contact

[dodhra.threatlab@mail.mil](mailto:dodhra.threatlab@mail.mil)

## Suggested Citation

Megill, L., VanBerschot, J., Kennedy, K., Van Note, Z., Chandler, C., & Rose, A. (2022). *Ensuring fairness and enhancing the protection of privacy in counter-insider threat programs: Resources and reflection activities*. (PERSEREC-PA-22-17, OPA Report No. 2022-177). Seaside, CA: Defense Personnel and Security Research Center/Office of People Analytics.



## Contents

<b>Introduction.....</b>	<b>4</b>
<b>Purpose.....</b>	<b>4</b>
<b>Organization .....</b>	<b>4</b>
<b>Resources to Get You Started .....</b>	<b>5</b>
<b>Case Studies.....</b>	<b>7</b>
<b>Case Study 1.....</b>	<b>7</b>
<b>Case Study 2.....</b>	<b>10</b>
<b>Case Study 3.....</b>	<b>13</b>
<b>The Ethical Decision-Making Process.....</b>	<b>16</b>
<b>Pause and Consider .....</b>	<b>17</b>
<b>Summary .....</b>	<b>18</b>
<b>Pause and Consider .....</b>	<b>18</b>
<b>Resources for Ethics in C-InT Work .....</b>	<b>19</b>
<b>Resources for Ensuring Fairness and Enhancing the Protection of Privacy.....</b>	<b>19</b>
<b>Relevant Policy.....</b>	<b>22</b>



## Introduction

Welcome to this collection of resources and reflection activities designed to help you think about how Counter-Insider Threat (C-InT) professionals can ensure fairness and enhance the protection of privacy in C-InT programs. Although individual departments and agencies have ethics officers to outline and provide specific guidance, there are no broadly applicable existing ethics and professional responsibility training or guides for U.S. Government C-InT programs.

This document is designed for anyone working in or supporting C-InT programs. The goal of the activities included is not to establish overall policy or create a generalizable framework, and the questions posed throughout this document do not have one “right” answer. Instead, this document provides an opportunity for you to respond to scenarios that incorporate ethical practices and protect the privacy of individuals in your work.

**When this document talks about ethics, it is referring to the principles that guide a C-InT program in protecting the dignity, privacy, and safety of the subject of an inquiry, other impacted individuals, and the organization.**

As you consider ethics in this context, it may also be useful to think about fairness, open-mindedness, trustworthiness, and the recognition and overcoming of biases.

## Purpose

The resources and activities included here are intended to encourage C-InT professionals to reflect on the ethical execution of their responsibilities. The questions and scenarios explored here are designed to provoke thought and inquiry, and the resources offer opportunities for further exploration of the topic. These resources and reflection activities can help you to think intentionally about how you might respond in challenging situations.

Consciously reflecting on low-stakes hypothetical scenarios can make you more aware of how to exhibit ethical decision making in real-life situations you may encounter. This awareness can ultimately contribute to ensuring C-InT programs are populated with people who are adept at adhering to and exhibiting ethical principles, which can lead to a more effective C-InT program, organizational trust (so employees of the organization are more likely to report), and better preparation for the future.

## Organization

This document begins with three **Case Studies** that provide opportunities to consider ethical decision-making in complex situations. Each case study includes:

- Case details
- Possible risk indicators
- Potential outcomes
- Questions to encourage reflection on how you might respond



The document then presents an **Ethical Decision-Making Process** that you can leverage to build the habit of making decisions guided by ethics. Finally, we conclude with a **Summary** reflection and a collection of **Resources for Ethics in C-InT Work** that you can use for further exploration of the topic.

### *Pause and Consider*

Throughout the reflection activities in this document you will see sections marked **Pause and Consider**. Review the questions found in these sections and consider how you or the organization could respond to mitigate the potential insider threat, without compromising ethical principles or the protection of privacy. Because there is no one correct answer to any of these questions, there is no answer key for the questions posed in these sections.

### Resources to Get You Started

There is no specific experience level required to utilize the reflection activities found here. Reflecting on specific, fictional scenarios and how to integrate ethical processes in daily work can benefit C-InT professionals at any level. However, we recommend you approach these activities with some knowledge of threat assessment, insider threat policy, and privacy and civil liberties. Before diving into the case studies provided here, you may find it helpful to review the two eLearning courses offered by the Center for Development of Security Excellence (CDSE) listed below,<sup>1</sup> particularly if you are new to the field.

Course	Description
Insider Threat Privacy and Civil Liberties INT260.16	<p>This course explains why civil liberties and privacy laws, regulations, and policies are so important in C-InT programs. Users will learn how to protect information, as well as what information is protected by law. Lessons contained in this training cover:</p> <ol style="list-style-type: none"><li>1. Privacy and Civil Liberties Guidelines</li><li>2. Civil Liberties and Insider Threat Programs</li><li>3. Insider Threat Challenges with Privacy and Civil Liberties</li><li>4. Balancing Institutional Protections and Individuals' Rights</li></ol> <p><b>Links:</b></p> <ul style="list-style-type: none"><li>• Course: <a href="https://www.cdse.edu/Training/eLearning-Courses/Insider-Threat-Privacy-and-Civil-Liberties-INT26016/">https://www.cdse.edu/Training/eLearning-Courses/Insider-Threat-Privacy-and-Civil-Liberties-INT26016/</a></li><li>• Student Guide: <a href="https://www.cdse.edu/Portals/124/Documents/student-guides/INT260-guide.pdf">https://www.cdse.edu/Portals/124/Documents/student-guides/INT260-guide.pdf</a></li></ul> <p><b>Length:</b> 90 minutes</p>

---

<sup>1</sup> These courses and links to additional supplemental materials can also be found in the **Resources for Ensuring Fairness and Enhancing the Protection of Privacy** section of this document.



Course	Description
Critical Thinking for Insider Threat Analysts INT250.16	<p>This course shows Insider Threat Analysts working in C-InT programs how to use visual and analytic techniques to create intelligence products without compromising the privacy and civil liberties of those involved. Lessons contained in this training cover:</p> <ol style="list-style-type: none"><li>1. Thinking for Insider Threat Analysts</li><li>2. Analytic Standards</li><li>3. Critical Thinking Tools</li></ol> <p><b>Links:</b></p> <ul style="list-style-type: none"><li>• Course: <a href="https://www.cdse.edu/Training/eLearning/INT250/">https://www.cdse.edu/Training/eLearning/INT250/</a></li><li>• Student Guide: <a href="https://www.cdse.edu/Portals/124/Documents/student-guides/INT250-guide.pdf">https://www.cdse.edu/Portals/124/Documents/student-guides/INT250-guide.pdf</a></li></ul> <p><b>Length:</b> 90 minutes</p>

The information in these courses can support you in formulating your answers to the questions in the **Pause and Consider** sections included throughout this document. The student guides for these courses can be leveraged alongside these reflection activities as a refresher on and to provide access to specific policies and information that may prove useful as you move through this document.



## Case Studies

The following three case studies contain fictional scenarios<sup>2</sup> centered around ethical decision-making. The intention of these case studies is to foster reflection on how best to mitigate the risk of insider threat and protect the privacy and rights of the subject of an inquiry.

**INSTRUCTIONS: Place yourself in the shoes of the C-InT analyst assigned to these cases and consider how you would react in these circumstances.**



### Case Study 1

### Mitigating Bias and Focusing on Relevant information

#### Case Details

This fictional case study is focused on a government contractor who created a drama podcast on a workplace attack. It is designed to explore questions around ethically conducting inquiries without letting biases or irrelevant information impact the process.

#### *Subject of the Inquiry*

- Vanessa Spinoza is a government contractor who works in aircraft manufacturing. She mostly keeps to herself in completing her work and has not formed social or personal connections with her coworkers or superiors. She often argues with one colleague in particular, James Ortega, and questions Mr. Ortega's qualifications and judgment; she is unafraid to disagree in any forum, which has led to multiple heated confrontations with a variety of coworkers in meetings. Her initial disagreements with colleagues led to a verbal warning but were not written up.
- Ms. Spinoza received a write-up after a heated conversation that ended with her saying Ortega would "get what's coming to him."
- Ms. Spinoza also received a formal, written warning after multiple instances of cutting corners and disregarding safety policies in the interest of meeting deadlines.
- In her spare time, Ms. Spinoza recently launched a fictional, serialized drama podcast that tells the story of an underappreciated technician who loses her job and then engages in a workplace attack. As the episodes progress, the characters become increasingly transparent stand-ins for her real-life coworkers, with a particular focus on the character who is a clear representation of Mr. Ortega. The fictional attack is carefully planned and graphically laid out, and the story plays out like a fantasy rehearsal.
- Ms. Spinoza's colleagues, especially Mr. Ortega and her manager, are concerned that this podcast is an outline for an actual attack she may be considering, particularly when coupled with her history of confrontational and antisocial behavior in the workplace.

---

<sup>2</sup> These fictional case studies were inspired by the anonymized cases presented in *Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks*: <https://www.fbi.gov/file-repository/making-prevention-a-reality.pdf/view>



- An analyst previously reviewed the case and recommended that management make it clear to Ms. Spinoza that she had shared proprietary information and violated company policy regarding threatening behavior by producing the podcast. Ms. Spinoza was also asked to sign a contract that laid out behavioral expectations and consequences for not adhering to those expectations. Once the contract was signed, the problematic behaviors ceased. The initial analyst also recommended ongoing observation, including enhanced user activity monitoring.

#### *Analyst Perspective*

As an analyst working in the C-InT hub of the contracting agency, you have been assigned the continued observation of Ms. Spinoza's case by your manager.

- You familiarize yourself with the previous incidents of concern, including reviewing the podcast episodes in question and reading the write-ups Ms. Spinoza received and written statements from Mr. Ortega on Ms. Spinoza's past behavior.
- In reviewing the monitoring on Ms. Spinoza conducted by the previous analyst, you discover that eighteen months earlier, Ms. Spinoza had to attend court-ordered defensive driving traffic school. You look more closely at her history and identify multiple reckless driving tickets from before she came to work at the company five years ago, one where she rear-ended someone and two others for speeding.

#### ***Possible Risk Indicators***

- Ms. Spinoza's podcast indicates a possible fantasy rehearsal for an act of workplace violence.
- Ms. Spinoza's willingness to cut corners, including in documentation and information handling, and her hostile approach to her coworkers speak to a possible lack of regard on her part for the organization's assets and personnel.
- Ms. Spinoza's reckless driving might cast doubt on her judgment and attitude toward risk.

#### ***Potential Outcomes***

- If Ms. Spinoza feels persecuted needlessly by the company and the C-InT program, it could cement her old grievances and contribute to her continuing, resuming, or beginning planning an act of workplace violence in earnest.
- However, if genuine risk exists, ending the enhanced monitoring too early could prove catastrophic for the organization.







## Case Study 2

## Using Publicly Available Electronic Information

### *Case Details*

This fictional case study is focused on a retired Navy SEAL who begins exhibiting threatening behaviors and activity on social media. It is intended to explore questions around how to use publicly available electronic information, including social media, and how actions taken by the organization and C-InT hub may differ depending on whether speech is protected.

#### *Subject of the Inquiry*

- Albert Williams has worked as a cleared IT Specialist for the Navy for six years. Mr. Williams is a decorated former Navy SEAL who served ten years before being honorably and medically discharged due to a back injury sustained during one of his many combat deployments.
- Five months ago, Mr. Williams was passed over for a promotion that he felt he deserved and his contentious divorce was finalized.
- In the past few months Mr. Williams' behavior has grown more erratic and confrontational, and he's been involved in multiple verbal altercations with colleagues. After one recent incident, he agreed to attend counseling offered through the Employee Assistance Program, but he stopped going after only a few sessions.
- One of Mr. Williams' colleagues reported increasingly threatening, paranoid-sounding, and anti-government social media posts on Mr. Williams' personal pages. These posts centered on both Mr. Williams' ex-wife and his manager and included statements that his manager was monitoring him at home to "look for problems" and "report up the chain." Mr. Williams has also written posts claiming his divorce was caused by the people he works with turning his ex-wife against him. In these posts he indicated he would seek revenge against his coworkers. Finally, Mr. Williams posted his ex-wife's personal information online and encouraged people to harass her.
- Last week Mr. Williams and Andrew Kim —a coworker with whom Mr. Williams works closely — got into a heated argument that nearly grew physical. Mr. Kim said he was certain Mr. Williams would have punched him if their manager had not intervened.
- Mr. Williams' manager previously reported feeling threatened after arguments with Mr. Williams about his performance. She reported this most recent argument between Mr. Williams and Mr. Kim because of her increased concern related to Mr. Williams' erratic behavior.

#### *Analyst Perspective*

As an analyst working in the Navy C-InT Hub, you have been assigned Mr. Williams' case by your manager.

- You open an inquiry into Mr. Williams and find the social media posts in question, as well as other posts where Mr. Williams talks about excessive drinking. In addition, you find posts alluding to the use of other illegal substances, with one post indicating he may be using these substances while he's at work.



- You talk to Mr. Kim and discover that he did not report the nearly physical altercation because he doesn't want to get Mr. Williams in trouble, and he was hoping the relatively new behavioral issues would resolve on their own.
- As a trained interviewer, you talk to Mr. Williams' manager and discover that another colleague mentioned that Mr. Williams has recently been heard at work making expletive-laden statements about both his ex-wife and his manager, similar to the content of his online postings.
- You also discover that as part of his clearance investigation, Mr. Williams reported being voluntarily committed for psychiatric evaluation and treatment twenty years ago, when he was a minor, after an altercation with a family member.

### ***Possible Risk Indicators***

- Mr. Williams' level of paranoia seems to be increasing. He communicates anti-government views and expresses that his employer, whom he sees as a representative of government, is working against him.
- Mr. Williams' social media posts indicate his substance use is beginning to interfere with his quality of life and may be contributing to paranoid thinking.
- Mr. Williams attempted to "dox" his ex-wife by sharing her home address and phone number on social media and encouraging harassment.

### ***Potential Outcomes***

- If the information found in the inquiry is not handled appropriately, the result could be a successful lawsuit by Mr. Williams against the organization and the findings of the inquiry being discredited or thrown out.
- If Mr. Williams follows through on the concerning comments he's made regarding both his manager and his ex-wife, he could cause serious physical harm.



**Case Study 3****Supporting the Subject of an Inquiry*****Case Details***

This fictional case study is focused on a government security professional who is going through a divorce and begins referencing mass shootings at work. It is intended to explore questions around conducting ethical inquiries that treat the subject fairly while also taking concerns seriously; how you might apply information given to you; and how to support the subject during an inquiry.

***Subject of the Inquiry***

- Anthony Isaacs is a security professional working as a Federal civilian employee in a facility that contains a Sensitive Compartmented Information Facility, to which he has access.
- Several months ago, Mr. Isaacs lost a child custody dispute. In the time since losing custody of his children, Mr. Isaacs has begun to express displeasure with his work situation. Coworkers mentioned he had started complaining about the stress that the job put on him and was clearly placing some of the blame for his family situation on his employment. On multiple occasions, he expressed complaints about “the people in charge around here.”
- Mr. Isaacs was reported to the C-InT hub by one coworker who said that in the last month, Mr. Isaacs had repeatedly alluded to a recent mass shooting at a shopping mall. In doing so, Mr. Isaacs showed a clear understanding of the details of the event and a level of interest that his coworker found concerning.
- Shortly after, an intoxicated Mr. Isaacs went to his ex-wife’s home where they got into a heated argument outside the house that resulted in his being arrested for verbal assault. Ms. Isaacs said she was not concerned about Mr. Isaacs becoming violent and declined to pursue a restraining order.
- His arrest triggered a suspension of his clearance, pending a personnel security eligibility review. Mr. Isaacs’ was assigned to administrative, non-sensitive tasks for the duration of the review.
- When investigators asked Mr. Isaacs about his repeated referencing of the mass shooting, he said he was just interested in current events. When they looked at Mr. Isaacs’ work phone, they found additional notes and searches that seemed to confirm a general interest in current events.
- Mr. Isaacs has filed an appeal in the custody dispute. He is attending regular counseling as part of the terms of the proposed, updated agreement and has begun supervised visitation with his children.

***Analyst Perspective***

As an analyst working in the C-InT hub for the component, you have been assigned the inquiry into the case.

- You assess that Mr. Isaacs’ current threat level is low, but due to his recent criminal conduct, Mr. Isaacs’ clearance was suspended. The personnel security eligibility review concluded, resulting in Mr. Isaacs’ clearance being revoked. Consequently, his manager has made the decision to terminate Mr. Isaacs’ employment.
- The manager asks you for mitigation recommendations on how best to handle the situation to preserve Mr. Isaacs’ dignity while avoiding creating additional risks as a result of his termination.



### ***Possible Risk Indicators***

- Mr. Isaac's recent behavior has resulted in criminal charges that led to his clearance being revoked.
- Mr. Isaacs' intoxication at the time of arrest raises concerns about the level and frequency of his alcohol consumption.
- Mr. Isaacs' current position and previous clearance provided him access to protected information within his work environment. During the termination process, the organization needs to ensure that he does not mishandle information and that he isn't allowed access to classified information.

### ***Potential Outcomes***

- If not handled correctly, Mr. Isaacs' termination could deepen existing grievances and result in psychological damage.
- If his firing leaves him in a difficult financial situation with no attempts to ease the burden, he could be more likely to sell sensitive information or even attempt suicide.










## The Ethical Decision-Making Process

**We are faced with ethical dilemmas on a regular basis.** Making decisions that adhere to ethical standards and ethical principles can have organizational benefits, such as building trust in and credibility for a C-InT program, and personal benefits, such as living free from doubt. However, there may be situations where making the right choice comes at a personal or professional cost. You may experience regrets about your decision, but if you follow ethical standards and principles, you will have fewer doubts. This section presents a process you can apply to making ethical decisions, even in the face of potential costs.

The process shown here is one example that you can use when faced with an ethical dilemma. The “right” decision may not always be immediately obvious. If you cultivate a habit of using this process when you encounter a lower-stakes decision, it can help you make higher-stakes decisions when the need arises.

	<b>Define the ethical dilemma</b>	Make sure you have a clear and complete understanding of the situation at hand and that you can articulate the ethical dilemma you face.
	<b>Outline the various possible courses of action (COAs)</b>	Identify the courses of action (COAs) available to you in this dilemma and mentally walk through each. For example, COA 1 might be to follow protocol to address an issue within the appropriate management chain. If no action is taken, what would be your next COA? Remember to consider the COA of taking no action at all.
	<b>Consider the outcomes/ consequences of each COA</b>	Carry each COA through to its logical conclusion. What are the personal and professional consequences or outcomes for each COA?
	<b>Consider pros and cons, including rewards and costs for yourself and all other parties impacted (e.g., your family, your organization, your profession).</b>	Think about the costs and rewards for the COAs you are considering, not only for yourself, but also for all other impacted parties (e.g., your family, your organization, your profession).
	<b>Make a decision you can live with</b>	Don't get trapped in “paralysis by analysis.” You may never be able to gather all of the information you feel is necessary to comfortably make a choice. In some circumstances, you may seriously consider the COA of taking no action and consciously choose that COA. However, recognize that simply failing to decide upon a COA is a decision to <i>not</i> act. Ultimately, you must make a decision you can live with and go from there. It's possible you will experience regrets that you didn't act in a certain manner or make a certain choice, but, at the end of the day, can you look in the mirror and feel good about yourself?









## Resources for Ethics in C-InT Work

The resources included here are intended to help identify relevant resources and policies to help you better address issues of fairness, ethics, and privacy.

### Resources for Ensuring Fairness and Enhancing the Protection of Privacy

The resources below can help you recognize the facets of an organizational culture that empowers individuals to address issues of fairness, ethics, and privacy. The list includes relevant courses, videos, and podcasts, organized by type. These resources will increase your knowledge on how C-InT personnel can better protect individuals' privacy and adhere to ethical standards specifically, as well as how C-InT personnel can encourage and practice behaviors that lead to a healthy organizational culture in general.

Product	Description
<b>E-LEARNING:</b> Insider Threat Privacy and Civil Liberties (CDSE) INT260.16	<p>This course explains why civil liberties and privacy laws, regulations, and policies are so important in C-InT programs. Users will learn how to protect information, as well as what information is protected by law.</p> <p><b>Links:</b></p> <ul style="list-style-type: none"><li>• Course: <a href="https://www.cdse.edu/Training/eLearning-Courses/Insider-Threat-Privacy-and-Civil-Liberties-INT26016/">https://www.cdse.edu/Training/eLearning-Courses/Insider-Threat-Privacy-and-Civil-Liberties-INT26016/</a></li><li>• Student Guide: <a href="https://www.cdse.edu/Portals/124/Documents/student-guides/INT260-guide.pdf">https://www.cdse.edu/Portals/124/Documents/student-guides/INT260-guide.pdf</a></li></ul> <p><b>Length:</b> 90 minutes</p>
<b>E-LEARNING:</b> Critical Thinking for Insider Threat Analysts (CDSE) INT250.16	<p>This course shows Insider Threat Analysts working in C-InT programs how to use visual and analytic techniques to create intelligence products without compromising the privacy and civil liberties of those involved.</p> <p><b>Links:</b></p> <ul style="list-style-type: none"><li>• Course: <a href="https://www.cdse.edu/Training/eLearning/INT250/">https://www.cdse.edu/Training/eLearning/INT250/</a></li><li>• Student Guide: <a href="https://www.cdse.edu/Portals/124/Documents/student-guides/INT250-guide.pdf">https://www.cdse.edu/Portals/124/Documents/student-guides/INT250-guide.pdf</a></li></ul> <p><b>Length:</b> 90 minutes</p>



Product	Description
<b>VIDEO:</b> Changing Hearts & Minds or Missed Opportunity? The Extremism in the Ranks Stand-Down	In the Spring of 2021, the Department of Defense (DoD) conducted an “Extremism in the Ranks” case study stand-down to give individuals the opportunity to speak openly and to address beliefs and attitudes that may have contributed to the January 6 Capitol riots. In this video, Dr. Erik Helzer and Dr. Paul Lester summarize the stand-down’s structure and outcomes and discuss implications it may have for combatting extremism within the DoD. <b>Video:</b> <a href="https://vimeo.com/592888786/ec53478804">https://vimeo.com/592888786/ec53478804</a> <b>Length:</b> 24 minutes
<b>VIDEO:</b> It Takes a Village: Linking Organizational Culture–Climate to Insider Threat	Dr. Frank Greitzer, Mr. Michael Ingerick, and Dr. Brian Griepentrog discuss how an organization’s culture and climate can influence an employee, inevitably shaping the critical pathway they may take, and how assessing organizational culture and climate is foundational to insider threat prevention and mitigation. <b>Video:</b> <a href="https://vimeo.com/588493495/a41eed7a45">https://vimeo.com/588493495/a41eed7a45</a> <b>Length:</b> 18 minutes
<b>VIDEO:</b> Keynote #2: Overcoming Cognitive and Interpersonal Biases	Dr. Kirk Kennedy discusses how personal and environmental factors affect our ways of thinking and how we relate to or form biases about others. He ends by discussing how to overcome these biases. <b>Video:</b> <a href="https://vimeo.com/607564591">https://vimeo.com/607564591</a> <b>Length:</b> 58 minutes
<b>VIDEO:</b> A Survivor’s Journey: Dedicated to Resiliency and Emotional Survival while Living with PTSD	On February 16, 2012, retired Assistant Special Agent Perry Woo became a hero during an act of workplace violence at the Long Beach Federal building when he took lethal action against his colleague, an active shooter. Mr. Woo shares real life examples of the psychical and emotional symptoms of post-traumatic stress disorder (PTSD), how to care for others who may be experiencing PTSD, and the consequences that could arise if adequate help and resources aren’t provided. <b>Video:</b> <a href="https://vimeo.com/457086418">https://vimeo.com/457086418</a> <b>Length:</b> 31 minutes
<b>VIDEO:</b> What’s Preventing Prevention: The Link Between Trust and Reporting	Matt Doherty discusses the link between reporting workplace misconduct and trust within the organization. He discusses indicators to measure trust in an organization, how leaders can build trust, and the benefits to an improved culture of trust and transparency. <b>Video:</b> <a href="https://vimeo.com/593453122/800c7947bd">https://vimeo.com/593453122/800c7947bd</a> <b>Length:</b> 16 minutes



Product	Description
<p><b>PODCAST:</b> Cultural Acceptance of PTSD/Trauma within Military &amp; Law Enforcement Organizations</p>	<p>Those in the military and law enforcement workforce culture may be exposed to repeated violence/death. This can lead to Post Traumatic Stress Syndrome (PTSS), which, despite its occurrence, still carries a stigma in this setting. In this podcast, Perry Woo, a retired Assistant Special Agent in Charge with Homeland Security Investigations explains why.</p> <p><b>Podcast:</b> <a href="https://anchor.fm/threatlab/episodes/Cultural-Acceptance-of-PTSDTrauma-within-Military--Law-Enforcement-Organizations-e15dpba/a-a6970o4">https://anchor.fm/threatlab/episodes/Cultural-Acceptance-of-PTSDTrauma-within-Military--Law-Enforcement-Organizations-e15dpba/a-a6970o4</a></p> <p><b>Length:</b> 26 minutes</p>
<p><b>PODCAST:</b> FBI Whistleblower Mike German: Part I of a Whistleblower Network News (WNN) Exclusive Interview</p> <p>FBI Whistleblower Mike German: Part II of a WNN Exclusive Interview</p>	<p>Mike German, renowned as a whistleblower, was a special agent for the Federal Bureau of Investigation (FBI). During an undercover mission, he was made aware of unlawful wiretapping and brought it to his management’s attention. In this two-part podcast, Mr. German talks about his experience, how he was pushed out of his position for speaking up, and potential changes the FBI could make to promote diversity in their hiring practices.</p> <p><b>Part I:</b> <a href="https://whistleblowersblog.org/podcasts/fbi-whistleblower-mike-german-part-i-of-a-wnn-exclusive-interview/">https://whistleblowersblog.org/podcasts/fbi-whistleblower-mike-german-part-i-of-a-wnn-exclusive-interview/</a></p> <p><b>Part I Length:</b> 60 minutes</p> <p><b>Part II:</b> <a href="https://whistleblowersblog.org/podcasts/fbi-whistleblower-mike-german-part-ii-of-a-wnn-exclusive-interview/">https://whistleblowersblog.org/podcasts/fbi-whistleblower-mike-german-part-ii-of-a-wnn-exclusive-interview/</a></p> <p><b>Part II Length:</b> 55 minutes</p>
<p><b>PODCAST:</b> No Tolerance for Zero Tolerance</p>	<p>A variety of experts discuss the problems with a zero-tolerance policy in the workplace, including lack of reporting, and describe different methods to address serious issues.</p> <p><b>Podcast:</b> <a href="https://anchor.fm/threatlab/episodes/No-Tolerance-for-Zero-Tolerance-etpkke/a-a566j22">https://anchor.fm/threatlab/episodes/No-Tolerance-for-Zero-Tolerance-etpkke/a-a566j22</a></p> <p><b>Length:</b> 46 minutes</p>



## Relevant Policy

The policies and guidance documents below are commonly referenced when topics of ethics, fairness, and privacy emerge.

Resource	Summary	Link
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Federal regulation that provides privacy and security regulations for protected health information	<a href="https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf">https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf</a>
2004 9/11 Commission Report	Report detailing the events leading up to 9/11, the response to the attack, and ways to deter future attacks	<a href="https://govinfo.library.unt.edu/911/report/index.htm">https://govinfo.library.unt.edu/911/report/index.htm</a>
Executive Order 13587	Executive Order to enhance the security of classified networks and the responsible sharing and safeguarding of classified information	<a href="https://www.dni.gov/files/NCSC/documents/nittf/EO_13587.pdf">https://www.dni.gov/files/NCSC/documents/nittf/EO_13587.pdf</a>
The National Insider Threat Policy and Minimum Standards	Policy documentation that promotes the safety of classified information	<a href="https://www.dni.gov/files/NCSC/documents/nittf/National_Insider_Threat_Policy_Minimum_Standards.pdf">https://www.dni.gov/files/NCSC/documents/nittf/National_Insider_Threat_Policy_Minimum_Standards.pdf</a>
Privacy and Civil Liberties Oversight Board (PCLOB)	Oversight board that reviews the federal government's efforts to combat terrorism to ensure privacy and civil liberties are protected	<a href="https://www.pclob.gov/">https://www.pclob.gov/</a>
Freedom of Information Act (FOIA) website	Act established to provide transparency into government documents, allowing the public to request access to records such as letters, emails, and recordings	<a href="https://www.foia.gov/index.html">https://www.foia.gov/index.html</a>
U.S. Constitution and the Bill of Rights – National Archives Website	Framework of the Federal Government and the first 10 amendments that define citizens' and states' rights	<a href="https://www.archives.gov/founding-docs">https://www.archives.gov/founding-docs</a> (document can be found in the "America's Founding Documents" tab)



Resource	Summary	Link
Privacy Act of 1974	Code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals and is maintained in systems of records by federal agencies	<a href="https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1279">https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1279</a>
Systems of Records Notice (SORN)	Component-specific, Department-wide, and Government-wide notices issued when a Federal agency creates, modifies, or abolishes a system of records	<a href="https://www.osec.doc.gov/opog/PrivacyAct/PrivacyAct_SORNs.html#BOU">https://www.osec.doc.gov/opog/PrivacyAct/PrivacyAct_SORNs.html#BOU</a>
The Privacy Act Consent Rule Exceptions Job Aid	CDSE job aid listing Privacy Act exemptions for information sharing	<a href="https://www.cdse.edu/Portals/124/Documents/jobaids/insider/privacy-act-exceptions.pdf?ver=HJqi1xHVfiCHApS-sFi1vQ%3d%3d">https://www.cdse.edu/Portals/124/Documents/jobaids/insider/privacy-act-exceptions.pdf?ver=HJqi1xHVfiCHApS-sFi1vQ%3d%3d</a>
DoD Directive 5205.16, The DoD Insider Threat Program	Directive for DoD to develop and maintain an insider threat program	<a href="https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/520516p.pdf">https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/520516p.pdf</a>
National Industrial Security Program Operating Manual (NISPOM)	Manual explaining the rules for protecting classified information	<a href="https://www.federalregister.gov/documents/2020/12/21/2020-27698/national-industrial-security-program-operating-manual-nispom">https://www.federalregister.gov/documents/2020/12/21/2020-27698/national-industrial-security-program-operating-manual-nispom</a>
Department of Defense Industrial Security Letter 2016-02	Letter requiring contractors to establish and maintain an insider threat program	<a href="https://www.dcsa.mil/Portals/91/Documents/CTP/tools/ISL2016-02.pdf">https://www.dcsa.mil/Portals/91/Documents/CTP/tools/ISL2016-02.pdf</a>
The Principle of Confidentiality	CDSE job aid summarizing the Principle of Confidentiality established by the Office of the Director of National Intelligence Privacy and Civil Liberties Office	<a href="https://www.cdse.edu/Portals/124/Documents/jobaids/insider/principles-confidentiality.pdf?ver=ntZqVMXolImyngG34Nq75w%3d%3d">https://www.cdse.edu/Portals/124/Documents/jobaids/insider/principles-confidentiality.pdf?ver=ntZqVMXolImyngG34Nq75w%3d%3d</a>



Resource	Summary	Link
Why Threats of Violence are Not Protected	CDSE job aid citing case examples when threats of violence were not protected	<a href="https://www.cdse.edu/Portals/124/Documents/jobaid/insider/threats-violence.pdf?ver=PXfxAJPximTqogBSoXQgNg%3d%3d">https://www.cdse.edu/Portals/124/Documents/jobaid/insider/threats-violence.pdf?ver=PXfxAJPximTqogBSoXQgNg%3d%3d</a>