[INSERT AGENCY NAME HERE]

INSIDER THREAT AWARENESS BRIEFING

NITAM
National Insider Threat Awareness Month

NITAM
National Insider Threat Awareness Month

At the end of this brief, you will be able to:

1. **Explain the importance** of detecting and reporting potential insider threats
2. **Identify indicators** of insider threat behavior and procedures to report such behavior
3. **Describe methodologies** of adversaries to recruit trusted insiders and collect classified information
4. **Understand** counterintelligence and security reporting requirements

What is an Insider Threat?

The threat an **insider** will use her or his authorized access **wittingly** or **unwittingly**, to **do harm** to the national security of the United States, their organization, or themselves.

This can include damage through espionage, workplace/kinetic violence, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

NITAM
National Insider Threat Awareness Month

How does the damage occur?

Espionage: Intelligence activity directed towards the acquisition of information through clandestine means.

Unauthorized Disclosure: A communication or physical transfer of classified information to an unauthorized recipient.

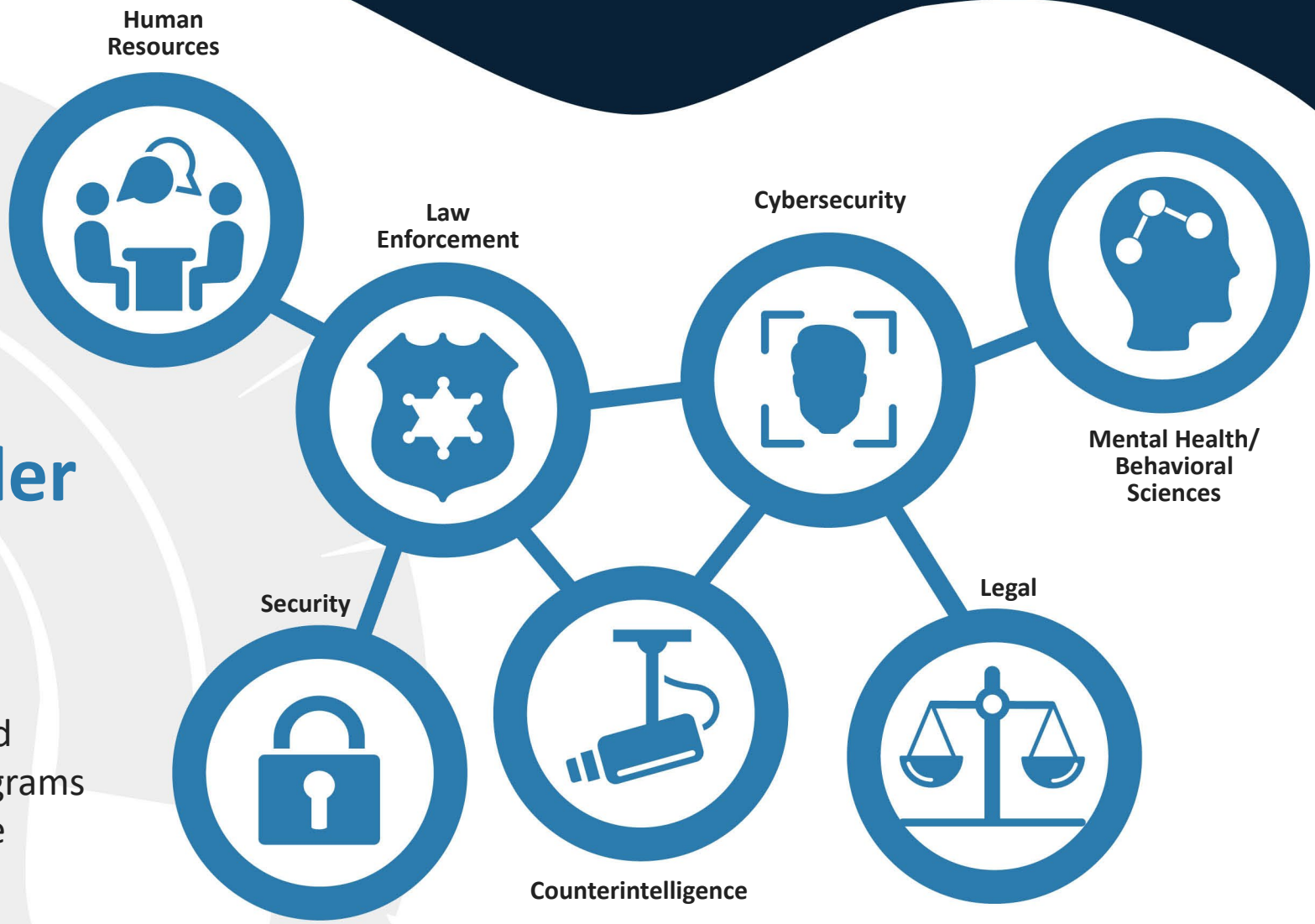
Workplace/Kinetic Violence: Any act of violent behavior, threats of physical violence, harassment, intimidation, bullying, verbal or non-verbal threat, or other threatening, disruptive behavior that occurs at or outside the work site, deliberate application of force to the human body with the intent to do harm.

NITAM
National Insider Threat Awareness Month

NITAM
National Insider Threat Awareness Month

How are Insider Threats mitigated?

Integrated Federal/DOD and Industry Insider Threat Programs (ITPs) with these seven core competencies:



DoD/Federal Agency Insider Threat Programs

- Executive Order 13587
- DoD Directive 5205.16
- National Insider Threat Policy and Minimum Standards

NITAM
National Insider Threat Awareness Month

National Industrial Security Program

- United States authority for managing the needs of private industry to access classified information
- 32 Code of Federal Regulations Part 117 National Industrial Security Program Operation Manual (NISPOM)

1. **All insider threat programs are required** to protect the privacy and civil liberties of the workforce.

2. **The lawful exercise of first amendment rights** and the use of legitimate whistleblowing channels to disclose fraud, waste, abuse or other questionable government activities are not considered actions of an Insider Threat.

3. Insider Threat Programs should **regularly consult legal counsel before taking action**.

NITAM
National Insider Threat Awareness Month

Who is the Insider Threat?

Opportunity + **Crisis** = **Vulnerability**

NITAM
National Insider Threat Awareness Month

NITAM
National Insider Threat Awareness Month

Unawareness

- Unknowingly committing security infractions or violations
- Misusing Government IT systems for non-work functions
- Discussing sensitive information in public
- Unknowingly clicking on a phishing scam

Complacency

- Using personal storage devices for official business without authorization
- Uploading sensitive files to a third a party site
- Allowing individuals without access into buildings or workspaces
- Unreported foreign contacts or travel
- Drug or alcohol use in the workplace

Malice

- Stealing sensitive information and sharing it for personal gain
- Threatening violence against self or peers
- Brandishing a weapon in the workplace
- Attempting to access information or space not relevant to the work assignment

NOTE: Exhibiting PRIs does not necessarily mean someone is a threat. However, most insider threats exhibit one or more PRI

Observable PRIs may fall into these categories:

- ⚠ Criminal, Violent or Abusive Conduct
- ⚠ Professional Lifecycle and Performance
- ⚠ Technical Activity
- ⚠ Unexplained Affluence
- ⚠ Judgement, Character and Psychological Conditions
- ⚠ Security and Compliance Incidents

NITAM
National Insider Threat Awareness Month

NITAM
National Insider Threat Awareness Month

Indicators in Context

The Critical Path, a theory developed by Dr. Eric Shaw and Dr. Laura Sellers

PERSONAL PREDISPOSITIONS + **STRESSORS** + **CONCERNING BEHAVIOR** + **PROBLEMATIC ORGANIZATIONAL RESPONSES** = **HOSTILE ACT**

Christopher Paul Hasson
Criminal, Violent or Abusive Conduct

Gabriel Romero
Professional Lifecycle and Performance

Shannon Stafford
Technical Activity

Candace Marie Claiborne
Unexplained Affluence

Ivan Lopez
Judgement, Character and Psychological Conditions

Henry Kyle Frese
Security and Compliance Incidents

NITAM
National Insider Threat Awareness Month

GABRIEL ROMERO

NITAM
National Insider Threat Awareness Month

PRIs:

Access Attributes — Romero was qualified for armed Topside Roving Patrol, which involves continuously walking the area around the submarine, and therefore had access to weapons.

Professional Lifecycle and Performance – Romero had been formally disciplined for repeated tardiness and dereliction of duty. He also had been passed over for promotion due to his failure to pass the Naval Advancement Exam.

Judgement, Character, and Psychological Considerations – Prior to the incident, Romero had not been diagnosed with a mental disorder, but the Force Psychologist did assess him with a "Phase of Life Problem" and an "Unspecified Problem Related to Unspecified Psychosocial Circumstances."

Impact:

Romero shot and killed two on-duty civilians and critically injuring another, and then killed himself while conducting Topside Roving Patrol on the USS Columbia at Pearl Harbor Naval Shipyard.

HENRY KYLE FRESE

NITAM
National Insider Threat Awareness Month

PRIs:

Security and Compliance Incidents:

- Accessed information outside his scope of job duties
- Provided classified national defense information via social media.
- Failed to report suspicious requests from individuals relating to classified national defense information

Impact:

Frese created risk of exceptionally grave harm to the security of the United States through unauthorized disclosure by repeatedly passing classified information at the TS/SCI level to journalists, who published that information, sharing it with all of the nation's adversaries.

SHANNON STAFFORD

NITAM
National Insider Threat Awareness Month

PRIs:

Declining work performance – Stafford's work performance in his new role was problematic, leading to demotion and, ultimately, dismissal.

Disgruntlement –Stafford was disgruntled over his demotion, which fueled his further decline in performance.

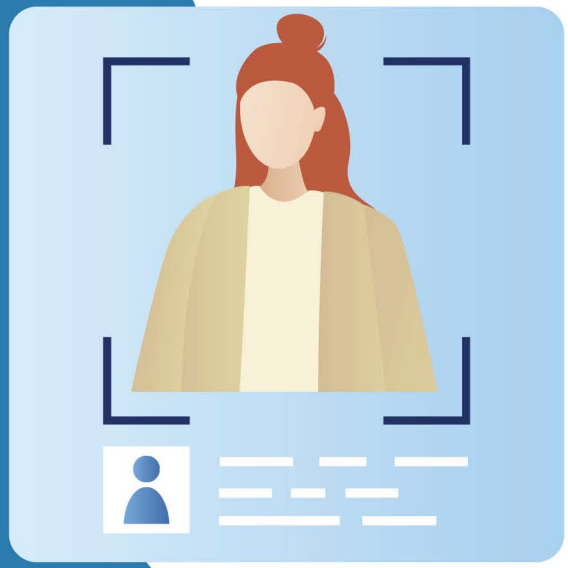
Technical Activity – Stafford had tried to access company data several times before he succeeded.

Access attributes – Stafford's position as an IT professional gave him the knowledge of other user's credentials

Impact:

Stafford's actions of deleting files and changing passwords to the storage management system caused severe disruption to the company's operations and the loss of some customer and user data. It also hindered the company's efforts to determine what happened and restore access to its remaining files. Stafford's damage and attempted damage to their computer systems, including the cost of restoring the deleted systems, investigating what happened, and responding to the intrusion, was at least $38,270.

CANDACE MARIE CLAIBORNE



PRIs:

Unexplained affluence, frequent unreported foreign contact, attempts to conceal foreign travel, frequent personal travel beyond known income

Impact:

Provided copies of internal documents from DoS on topics ranging from U.S. economic strategies to visits by dignitaries between two countries

NITAM
National Insider Threat Awareness Month

IVAN LOPEZ

PRIs:

Depression, anxiety, sleep disturbances, possible PTSD, recent deaths in the family, substandard performance, stressful PCS

Impact:

Wounded 14 other soldiers, killed three soldiers, left behind wife and children

NITAM
National Insider Threat Awareness Month

CHRISTOPHER PAUL HASSON

NITAM
National Insider Threat Awareness Month

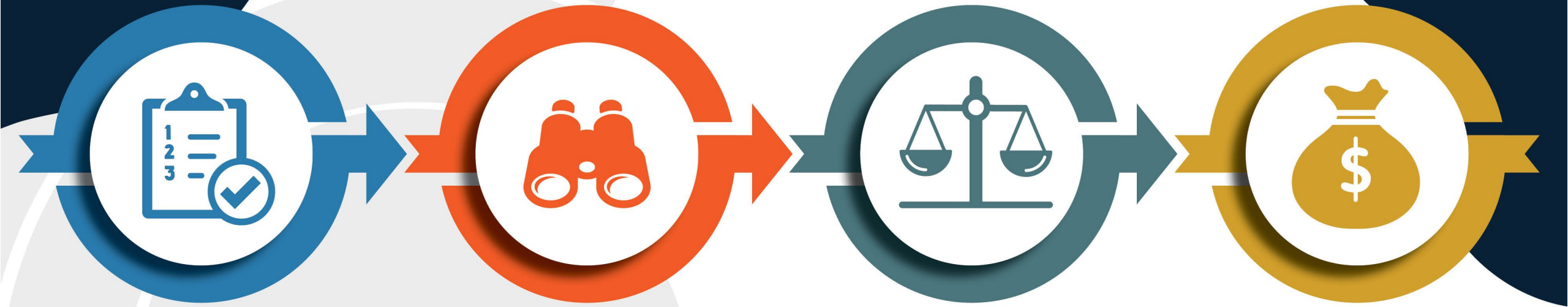
PRIs:

Association with extremist views, expressing ill will toward U.S. Government, Possessing illegal weapons and drugs, and misuse of U.S. Government automated information system

Impact:

This case exemplifies a positive insider threat outcome in that a hostile act was prevented by an effective insider threat program. Had his activities not been detected in time, he might have been able to carry them out against some individuals whom he researched and placed on target lists

NITAM
National Insider Threat Awareness Month



1 Identify & Prioritize Assets

2 Examine Threat Environment

3 Assess Vulnerabilities

4 Gauge Cost of Asset Loss

NITAM
National Insider Threat Awareness Month

1. **Spot & Assess**
2. **Develop**
3. **Recruit**
4. **Elicit**

NITAM
National Insider Threat Awareness Month

DOD REPORTING

- ✓ **DoD Directive 5240.06 Counterintelligence Awareness and Reporting (CIAR) requires reporting contacts, activities, indicators and behaviors associated with foreign intelligence entities**
- ✓ **DoDD 5205.16 requires reporting of Insider Threat Indicators**
- ✓ **Immediately report suspicious activities, behaviors, and contacts to your supervisor, security, or insider threat program personnel**

NITAM
National Insider Threat Awareness Month

INDUSTRY REPORTING

- ✓ **Report any incidents that meet thresholds of 32 CFR Part 117 NISPOM, section 117.8. These include adverse information, security violations, personnel security issues, and suspicious contacts**
- ✓ **Cleared contractors must also report actual, probable or possible espionage, sabotage, terrorism or subversion to both the Federal Bureau of Investigation (FBI) and Defense Counterintelligence & Security Agency (DCSA)**
- ✓ **Immediately report suspicious activities, behaviors, and contacts to your supervisor, facility security officer, or insider threat program**

NITAM
National Insider Threat Awareness Month

FAILURE TO REPORT

DoD personnel who fail to report are subject to judicial or administrative action (or both) pursuant to applicable law and regulations.

- **UCMJ: Punitive action under article 92**
- **Civilian employees: appropriate disciplinary action under regulation governing civilian employees**

Industry personnel who fail to report are subject to disciplinary action (including termination), fines, prison, or a combination of all three

AWARENESS IS KEY

National Insider Threat Awareness Month

NITAM
National Insider Threat Awareness Month

Agency SOP:
[NAME and LOCATION]

Insider Threat Reporting POC:
[NAME and CONTACT INFO]

Security POC:
[NAME and CONTACT INFO]

Counterintelligence Reporting POC:
[NAME and CONTACT INFO]

NITAM
National Insider Threat Awareness Month

You should now be able to:

- ✓ **Explain the importance** of detecting and reporting potential insider threats
- ✓ **Identify indicators** of insider threat behavior and procedures to report such behavior
- ✓ **Describe methodologies** of adversaries to recruit trusted insiders and collect classified information
- ✓ **Understand** counterintelligence and security reporting requirements