

DETER, DETECT, MITIGATE

SEPTEMBER 2024 NATIONAL INSIDER THREAT AWARENESS MONTH BRIEFING

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

***Unclassified – Prepared for Public Release ***





INTRODUCTION – Insider Threat Timeline

This timeline represents some, but not all, of the major violent events, unauthorized disclosures, and policies for insider threat since 2010.



FEB 2010

Chelsea Manning sends first of hundreds of thousands of leaked documents to Wikileaks



MAY 2013

Edward Snowden begins leaking classified documents to the Washington Post

The 2017 National Defense Authorization Act defines an insider threat for the Department of Defense as, “a threat presented by a person who has, or once had, authorized access to information, a facility, a network, a person, or a resource of the Department and wittingly, or unwittingly, commits an act in contravention of law or policy that resulted in, or might result in, harm through the loss or degradation of government or company information, resources, or capabilities; or a destructive act, which may include physical harm to another in the workplace.”



SEP 2013

Aaron Alexis commits active shooter event at Washington Navy Yard



APR 2014

Ivan Lopez commits active shooter event at Fort Hood



MAY 2017

Reality Winner sent Top Secret classified information to a news reporter



Major Kinetic Violent Insider Threat Event



Major Unauthorized Disclosure



Major Policy Update or Response



NOV 2011

Executive Order 13587 establishes requirements for insider threat programs



NOV 2012

National Minimum Standards for Department/ Agency insider threat programs established



FEB 2014

DITMAC established



DEC 2019

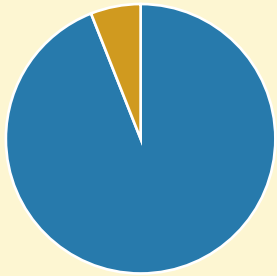
Gabriel Romero commits active shooter event at Pearl Harbor Naval Shipyard



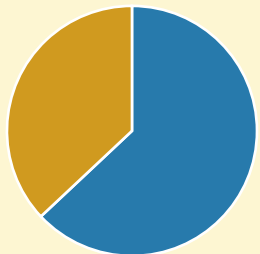
DETER - Organizational Culture: Common Challenges



Stress



94% of American workers experience stress at their workplace.



63% considering quitting due to stress-related issues



Perceptions of Justice and Fairness



Employees who perceive their workplace as unjust are **4.6 times** more likely to engage in insider threat behaviors than those who feel their organization is fair and just



Communication



Poor communication fuels grievances and may lead to disgruntlement, hostile attitudes, decreased productivity, low morale, and can ultimately hinder mission readiness.



DETER - Organizational Culture: Best Practices

Individual / Servicemember Best Practices



Officer, NCO, and Supervisor Best Practices



Manage Stress

Develop Healthy Responses

Encourage Healthy Responses

Track Stressors

Model Best Practices

Seek Support from Family, Friends, Colleagues, and/or Professionals.

Encourage Seeking Help and Offer Support

Communicate with Chain of Command/ Supervisor

Know and Understand Your People

Maintain Healthy Boundaries

Offer Flexibility When Possible

Source: ["Coping with stress at work" \(apa.org\)](#), July 2014.



Ensure Fairness

Share Information When Permissible

Keep Employees Informed

Support Your Coworkers

Promote Awareness of Resources

Discuss Career Opportunities and Advancement

Ensure Fairness for Internal Opportunities

Recognize Coworker Contributions

Recognize Employee Contributions

Discourage Bad Behaviors

Hold Employees Accountable

Source: Kropp, Brian, Jessica Knight, and Jonah Shepp. "How Fair is Your Workplace." Harvard Business Review, 14 July 2022. [Link](#).



Communicate Effectively

Be Clear and Concise

Promote 2-way Communication

Practice Active Listening

Respond to Servicemember / Employee Input

Understand Communication Systems

Specify Preferred Communication Channels

Understand and Assess Yourself and Your Actions

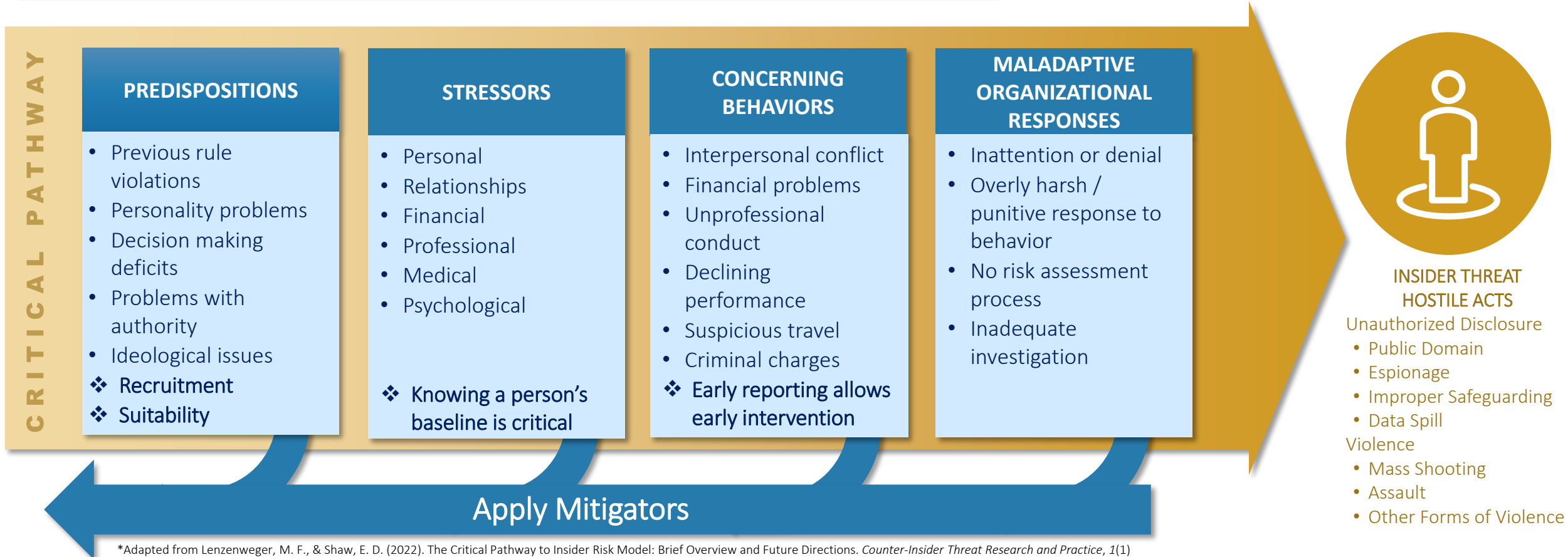
Understand and Assess Yourself and Your Actions

Source: Emerson, Mary Sharp. "8 Ways You Can Improve Your Communication Skills." Harvard Business Review, 30 August 2021. [Link](#).



DETECT – The Critical Pathway

The Critical Pathway provides a framework for examining the various factors that can contribute to risk for possible future insider threat hostile acts.





MITIGATE – Apply Critical Pathway Mitigators

CRITICAL PATHWAY

PREDISPOSITIONS

STRESSORS

CONCERNING
BEHAVIORS

MALADAPTIVE
ORGANIZATIONAL
RESPONSES



Mitigators are ways to help someone get off the critical pathway or prevent someone from starting along the pathway

Apply Mitigators

COUNTERBALANCE PREDISPOSITIONS

- Training
- Consider Recruiting for Security Eligibility
- Evaluate Behavioral Patterns and Changes
- Embrace Security Culture
- Take Personal Responsibility

RELIEVE AND MANAGE STRESSORS

- Educate About Stress Reduction
- Encourage Benefits Utilization
- Provide Resources for Support
- Combat Harmful Stigma
- Assess the Risk
- Understand and Use Positive Coping Strategies
- Manage and Mitigate Risk

REACT TO CONCERNING BEHAVIORS

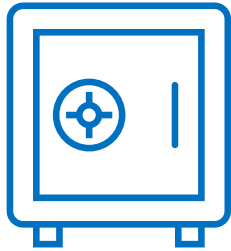
- Tailor Active Management over time
- Acknowledge Disgruntlement
- Address Grievances
- Impose Logical Consequences
- Set Performance Improvement Plan
- Investigate Concerning Behavior
- Enhance Technical Monitoring
- Conduct a Behavioral Science Assessment
- Suspend Access and/or Terminate Employment
- Reward Positive Behaviors
- Document/Track Enterprise Risk

DEVELOP APPROPRIATE ORGANIZATIONAL RESPONSES

- Take Timely Action
- Remove Logical and Physical Access
- Harden Defenses
- Secure Resources
- Protect People
- Detain or Arrest
- Prosecute and/or UCMJ
- Prevent Transfer of Risk
- Component and DITMAC insider threat multidisciplinary teams of experts can support



MITIGATE – Reporting Insider Threats



Safeguard



Contact Security



Contact Insider Threat



Intentional or Inadvertent

Reporting is required whether the action is intentional or inadvertent.



Physical or Virtual

Reporting is required for actions regardless of whether they take place online or physically / in person.



Yourself or Another

Reporting is required whether the action was performed by yourself or someone else.



DITMAC DOD Insider Threat Management and Analysis Center

DITMAC Reporting Portal

The DITMAC's reporting portal allows anyone to submit an anonymous report directly to the DITMAC team. Our multidisciplinary team will work with components to validate and coordinate our efforts.

<https://ditmac.experience.crmforce.mil/reporting>



CONCLUSION



DITMAC COMMUNICATIONS

DITMAC Communications
Office
dcsa.quantico.dcsa.mbx.ditmac-communications@mail.mil



2024 DCSA NITAM CONFERENCE

SEP 9th and 10th
in Arlington, VA
or online. Register at:
https://dcsa.acms.com/nitamconference2024/event/event_info.html



INSIDER THREAT ONLINE TRAINING

Cdse.usalearning.gov, and
sign up for
their newsletter here:
<https://www.cdse.edu/Cdse-News/>



AFTER ACTION REPORT

Please fill out our AAR
survey
[Link to Survey](#)



Sign up for the monthly BTAC Bulletin for Insider Threat evidence-based topics @ dcsa.quantico.dcsa.list.ditmac-sme@mail.mil or at [www.https://DCSA.mil/DITMAC](https://DCSA.mil/DITMAC)