

Insider Threat and the Effects of COVID-19

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY





VIRTUAL ROOM SETUP

Enlarge Screen



File Share



Closed
Captioning
below



Q & A





YOUR THOUGHTS - FEEDBACK

At the end of our event, please take a few minutes to share your opinions

Your feedback helps us improve the quality of our offerings.

Responding will only take a few minutes.

Responding is optional.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE WEBINAR FEEDBACK

OMB CONTROL NUMBER: 0704-0553

Expiration: 3/31/2022

The public reporting burden for this collection of information, 0704-0553, is estimated to average 3 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or burden reduction suggestions to the Department of Defense, Washington Headquarters Services at whs.mcalex.esd.mbx.dd-dod-information-collections@mail.mil. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.



INTRODUCTIONS

HOSTS:

Dr. Brad Millick

OUSD(I&S) Insider Threat Program Manager

Ms. Delice Bernhard

Director, DOD Insider Threat Management and Analysis Center (DITMAC)

Ms. Rebecca Morgan

Deputy Assistant Director, Insider Threat, National Counterintelligence and Security Center (NCSC)

Deputy Director, National Insider Threat Task Force (NITTF)



AUDIENCE POLL QUESTION # 1

Multiple Choice:

How many TV series have you binged in the last year?

- a. Less than 10
- b. More than 10
- c. More than 20(!)
- d. None: My kids have had Sponge Bob on a constant loop



AGENDA

- Unique Risk Environment
- Insider Threat Challenges
- Mitigation Opportunities
- Turning for Help/Resources
- Adjusting for the New Normal





AUDIENCE POLL QUESTION # 2

True or False:

There are no insider threats in a telework-only environment.

- a. TRUE
- b. FALSE

UNIQUE RISK ENVIRONMENT





INSIDER THREAT CHALLENGES



COVID-19 UPDATE
SCHOOLS CLOSED



MITIGATION OPPORTUNITIES





AUDIENCE POLL QUESTION # 3

True or False:

I have access to resources to support myself and my staff through challenging times.

- a. TRUE
- b. FALSE

RESOURCES



COVID and Burnout

<https://hbr.org/2021/02/beyond-burned-out>



Resilience

<https://www.cdse.edu/toolkits/insider/resilience.html>





RESOURCES

Continuity of Operations Planning

<https://www.fema.gov/disasters/coronavirus/rumor-control>

Coronavirus Resources

<https://www.fbi.gov/coronavirus>

<https://www.justice.gov/coronavirus>

<https://www.coronavirus.gov/>

https://www.cdc.gov/coronavirus/2019-ncov/communication/social-media-toolkit.html?fireglass_rsn=true



AUDIENCE POLL QUESTION # 4

How Do You Feel About the “New Normal”?

- a. Nothing—I feel normal about It
- b. Half-baked—hybrid school, hybrid work, hybrid life
- c. Readjusted and rolling With It
- d. Sweatpants FOREVER!

ADJUSTING FOR THE NEW NORMAL



QUESTIONS

UNCLASSIFIED

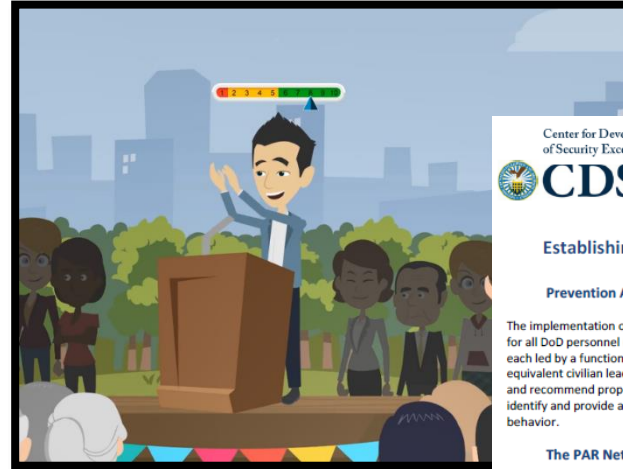


UNCLASSIFIED



NEW INSIDER THREAT TRAINING & AWARENESS PRODUCTS

- Graphic Novel
 - [“Dangerous Disclosure”](#)
- Security Training Video
 - [Resilience Animation](#)
- Tool Kits
 - Critical Infrastructure
 - Building Resilience
- Job Aids
 - [Establishing Prevention, Assistance, and Response \(PAR\) Capabilities](#)
 - Behavior Science in Insider Threat



Center for Development of Security Excellence
 **CDSE** **INSIDER THREAT JOB AID** LEARN. REFLECT. PROTECT.

Establishing Prevention, Assistance, and Response (PAR) Capabilities

Prevention Assistance Response (PAR) Capability

The implementation of PAR capabilities applies to the DoD Enterprise and seeks to create a safer environment for all DoD personnel (military and civilians). PAR capabilities represent a network of multi-disciplinary efforts, each led by a functional expert operating at the installation level. These experts assist commanders and their equivalent civilian leaders define the risk to DoD personnel, organizations, installations, or separate facilities and recommend proportional responses to mitigate or eliminate this risk. Furthermore, PAR capabilities identify and provide assistance and remedies to organizational personnel at risk for potentially violent behavior.

The PAR Network

What constitutes a network of multi-disciplinary efforts? In real terms, PAR capabilities are dictated by the resources and expertise available to the installation leadership. In the optimum situation, PAR capabilities encompass many, if not all, of the following areas: legal; military and civilian personnel management; defense contract administration; chaplain; military criminal investigative organizations; family advocacy; suicide prevention; sexual harassment and assault; drug and alcohol programs; mental health; law enforcement; physical, personnel, industrial, and information security and assurance, including digital information protection; and privacy program. Each advisor shall be an expert in their field and certified as one in accordance with departmental or Component standards. The principal goal is to leverage and synchronize existing personnel support programs and processes into a comprehensive effort, using onboard functional experts to advise the installation commander or civilian equivalent. Components, installations, and facilities that have PAR-like capabilities in place and are operational are not required to establish a separate set of duplicative capabilities.

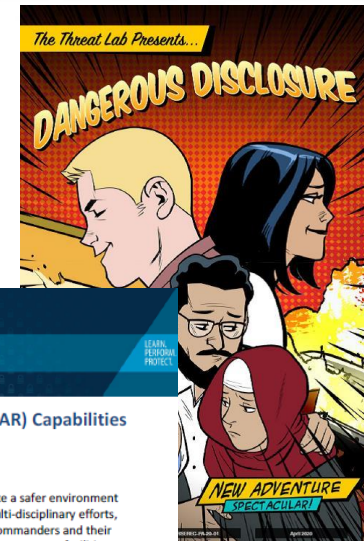
PAR Implementation Goals

Goal 1: Provide information and advice to installation Commanders and Equivalent Civilian Leaders to fully inform their risk or threat assessment(s).

Goal 2: Integrate PAR capabilities at the Installation with Component programs focused on deterring, detecting, and preventing threats from insiders.

Goal 3: Promote and facilitate information sharing to collect and analyze relevant data from authorized sources.

Goal 4: Render support to employees who are victims of or impacted by violence; and provide assistance and referrals to support programs.



VIGILANCE CAMPAIGN MATERIAL



[Insider Threat Vigilance Campaign 2021](#)

Insider Threat Vigilance Video Series, Season 2

Episode 1: [Organizational Trust](#)

Episode 2: [Indicators](#)

Episode 3: [If You See Something, Say Something](#)

Episode 4: [Outcomes](#)

VIEW MORE MATERIAL HERE:

<https://www.cdse.edu/toolkits/insider/vigilance.html>

INSIDER THREAT VIGILANCE CAMPAIGN 2021

A vigilance campaign helps implement Insider Threat Awareness training. Select a month or create your own campaign with resources from our [website](#).

JANUARY Mental Health	JULY Positive Outcomes
FEBRUARY Cultural Awareness	AUGUST Unintentional Threats
MARCH Organizational Trust	SEPTEMBER Insider Threat Awareness
APRIL Prevention Assistance Response	OCTOBER Cybersecurity Insider Threats
MAY The Critical Path	NOVEMBER Infrastructure & Resilience
JUNE Insider Threat Programs	DECEMBER Privacy & Civil Liberties

CDSE Center for Development of Security Excellence

LEARN. PERFORM. PROTECT.



SUBSCRIPTION SERVICE

Sign up to get the latest CDSE news and updates delivered straight to your inbox!

ABOUT CDSE

- Awards
- Customer Base
- Frequently Asked Questions
- History
- Information for Visitors
- Mission/Vision
- News
- Products and Services
- Professional Affiliations
- Year End Reports

ABOUT THIS SITE

- A-Z Listing of Terms
- Accessibility/Section 508
- Disclaimer
- FOIA
- Information Quality
- No FEAR Act
- Open GOV
- Plain Writing Act
- Privacy Policy
- Sitemap
- USA.gov

CONNECT

- Contact CDSE
- Follow us on Twitter
- See us on YouTube
- Subscribe to our RSS Feeds
- Visit us on Facebook

NEWSLETTER

Sign-up for emails from CDSE to get the latest news and updates in your inbox.

Enter your email address

Submit



<https://www.cdse.edu/news/index.html>



CDSE INSIDER THREAT SENTRY APP

MOBILE APPLICATION FOR ANDROID AND IPHONE

Available in iTunes App Store and Google Play (no cost to user).



SOCIAL MEDIA



Make sure to check out our social media accounts!



CDSE – Center for
Development of
Security Excellence

*Like our page on
Facebook!*



@TheCDSE

*Follow us on
Twitter!*



Center for
Development of
Security Excellence

*Subscribe to our
channel on YouTube!*



UPCOMING CDSE WEBINARS

Date	Title
April 14	Meet the DITMAC: An Overview of Analysis & Mitigation, Enterprise Program Management Office, Unauthorized Disclosure Program Management Office, and Performance & Metrics.
July 29	Organizational Culture and Countering Insider Threats: Best Practice Examples from the Marine Corps Insider Threat Hub
September 2	Insider Threat Virtual Conference

For more information and to register for these webinars, visit <https://www.cdse.edu/catalog/webinars/index.html>



CDSE WANTS TO HEAR FROM YOU



Insider Threat Training POC:

Steven D. Resel

(410) 689-1135

Email: steven.d.resel.civ@mail.mil

Insider Threat Training Mailbox:

dcsa.cdsetraining@mail.mil