INSIDER THREAT DIVISION

CENTER FOR DEVELOPMENT OF EXCELLENCE

FOOD DEFENSE CONSORTIUM

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

CDSE

INSIDER RISK AWARENESS

Rebecca Morgan, Chief, Insider Threat Division
Center for Development of Security Excellence
Defense Counterintelligence and Security Agency

INSIDER RISK AWARENESS

- I Don’t Need an Insider Threat Program
- It’s Too Difficult to Establish an Insider Threat Program
- I Don’t Have the Expertise to Run an Insider Threat Program
- I Can’t Afford an Insider Threat Program

Defining Insider Threat

Insider

Anyone with authorized access.

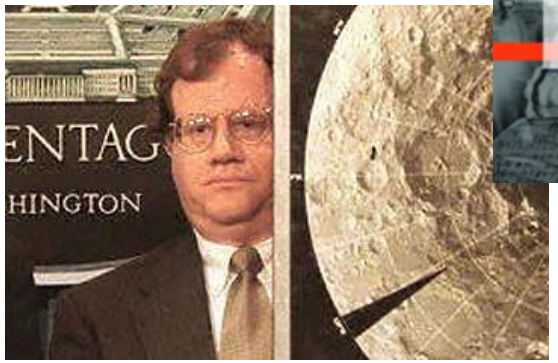
Defining Insider Threat

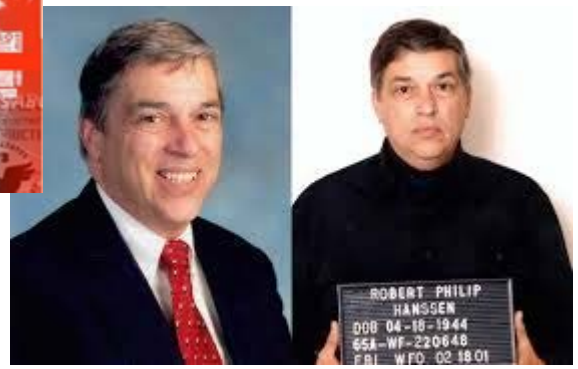
Insider Threat

The likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to an organization, including the loss or compromise of information, facilities, and personnel.

INSIDER RISK AWARENESS

Defining Insider Threat

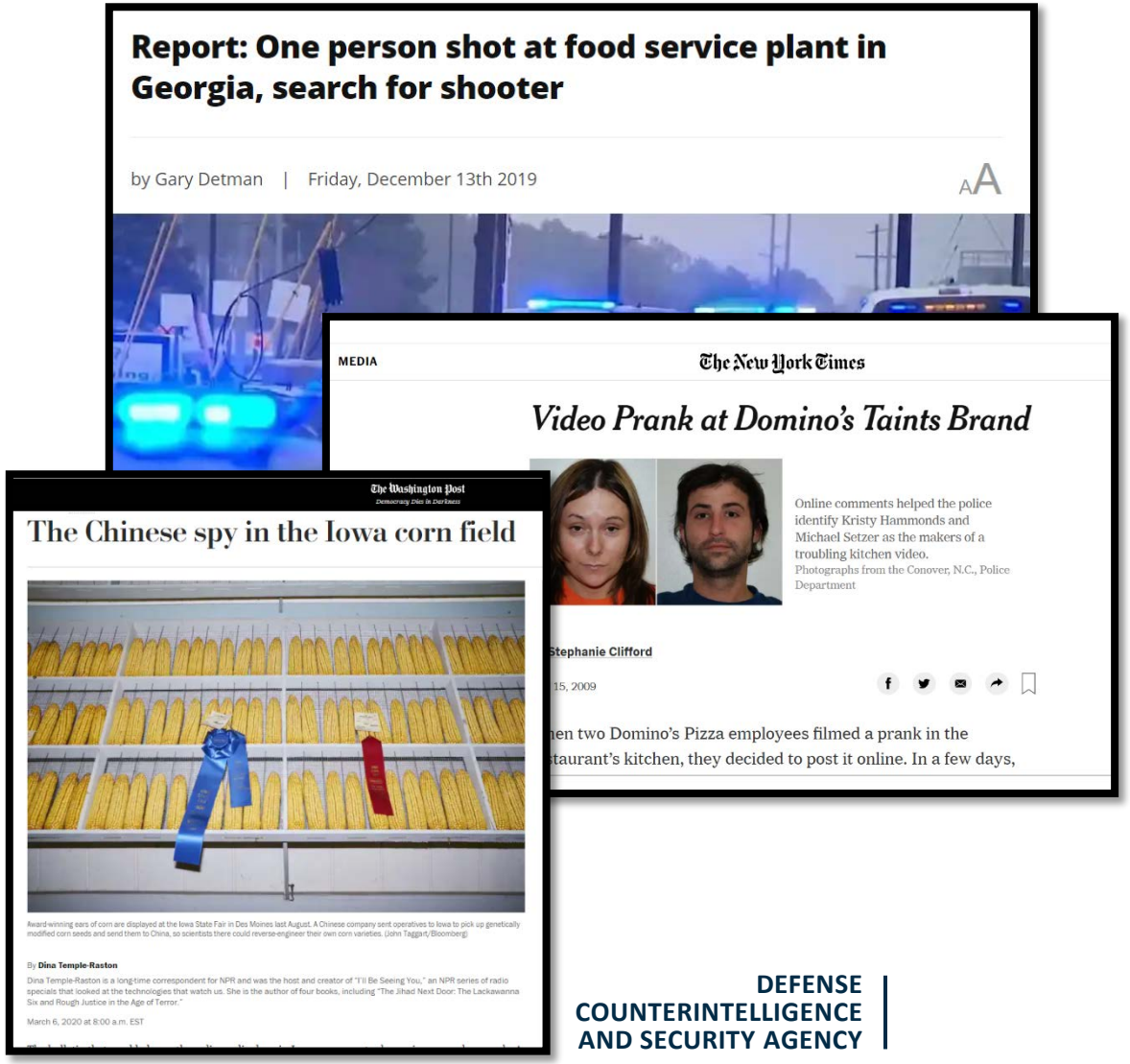




INSIDER RISK AWARENESS

Insider Threats in Food and Agriculture Sector

- Food Adulteration
- Contamination
- Data Breach
- Fraud
- Theft
- Sabotage
- Loss of Trade Secret or Proprietary Data
- Tainted Supply Chains
- Acts of Violence



DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Witting and Unwitting Insiders

Factors Contributing to Vulnerability

Opportunity and crisis contribute to vulnerability.

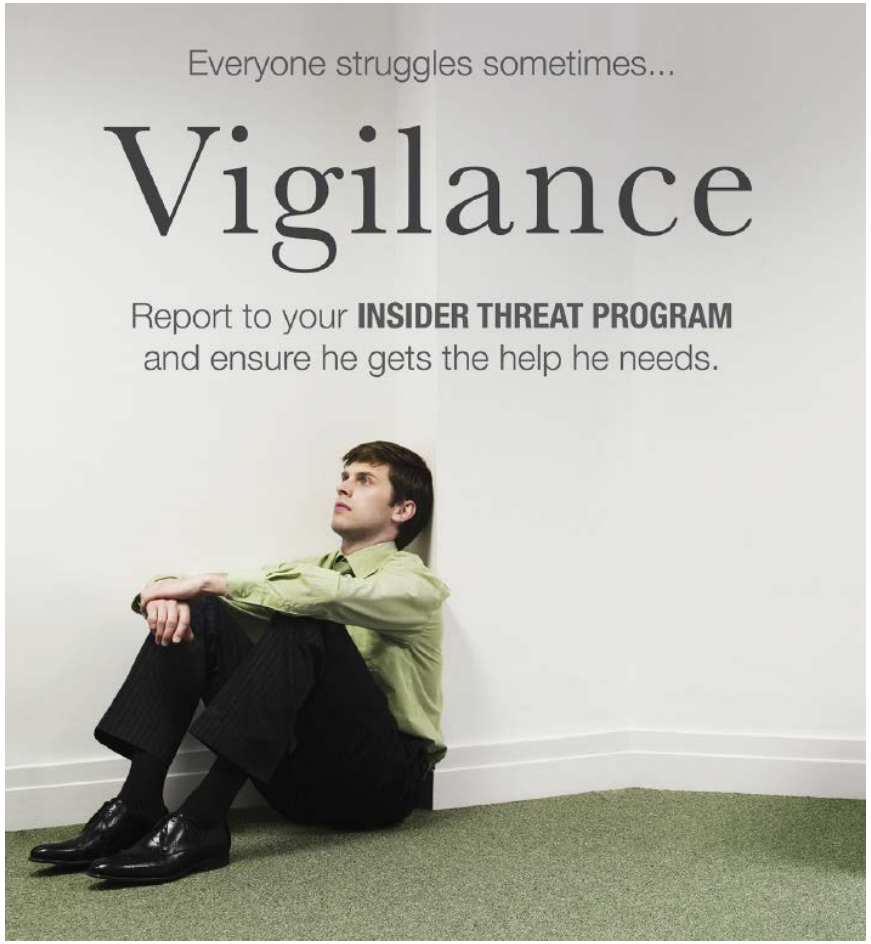
Potential Risk Indicators (PRIs)

Most employees engaging in negative behavior showed one or more PRIs.

- Access Attributes
- Professional Lifecycle and Performance
- Foreign Considerations
- Security and Compliance Incidents
- Technical Activity
- Criminal, Violent, or Abusive Conduct
- Financial Considerations
- Substance Abuse and Addictive Behaviors
- Judgement, Character, and Psychological Conditions

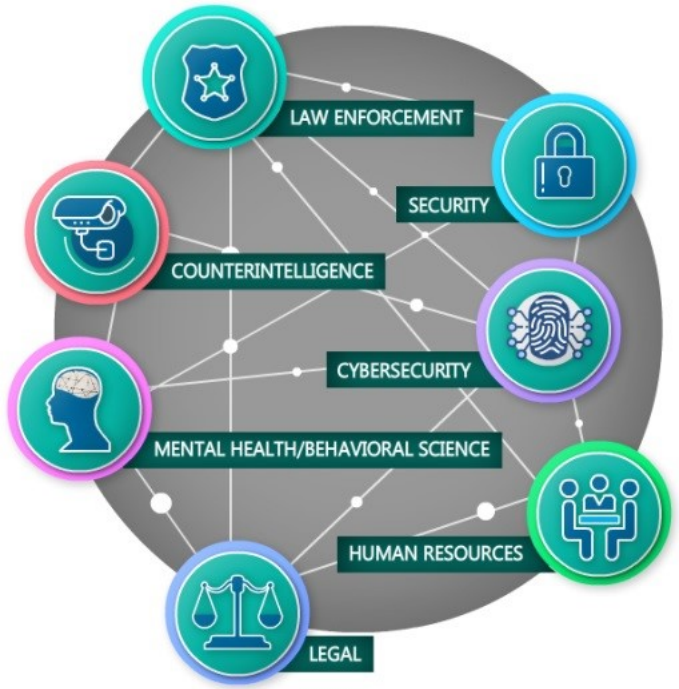
See something, say something!

INSIDER RISK AWARENESS



Insider Risk Programs

- ❑ **Multidisciplinary** Teams
- ❑ **Proactive**ly Deter, Detect, and Mitigate Risk
- ❑ Respect the **Privacy** and Civil Liberties of the Workforce
- ❑ Seek **Positive** Outcomes
- ❑ Manage Risk to **Protect** Organizations and their Resources



Resources

INSIDER RISK AWARENESS

ESTABLISH your insider risk program by working with senior leadership to designate a senior official or program manager. Work with senior managers from throughout your company including security, human resources, legal, and information technology representatives to craft an Insider Risk Program Plan and establish information sharing policies and mitigation strategies. Conduct a Risk Assessment to identify critical assets, threats to your organization, unique vulnerabilities, and appropriate countermeasures to address the insider threat.

DETER insider threat activities and manage insider risk by instituting training and awareness programs for all personnel. Ensure that principles of organizational trust, fairness, and transparency are part of your work culture and communicated to employees. Evaluate work processes and security protocols such as pre-employment vetting, principle of least privilege, separation of duties, and termination procedures to ensure that insider risk considerations are in place.

DETECT behaviors and activities indicative of potential risk by encouraging reporting to front line managers, supervisors, human resources, security and insider risk program personnel. Consider establishing designated email and/or phone lines and ensure employees know what to report and to whom. Establish user activity monitoring capability on sensitive systems or those that house proprietary data.

INSIDER RISK AWARENESS

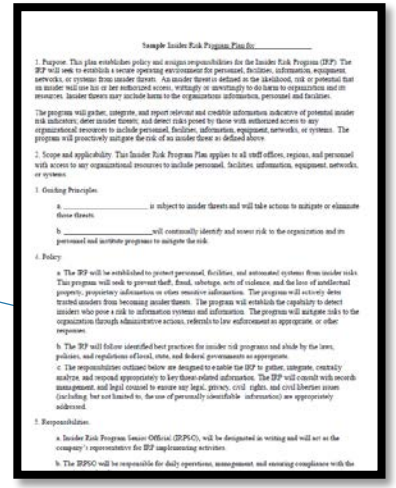
MITIGATE potential risk by addressing insider risk indicators early – before a negative event occurs. Coordinate with your multidisciplinary insider risk team to deploy proactive interventions. Many risks can be mitigated with increased training, updated security protocols, or human resources and employee assistance program strategies. Decide how the team will handle indicators and ensure fair, consistent application of mitigation strategies.

REFER insider threat incidents and/or potential risk indicators that cannot be resolved to appropriate local and federal law enforcement. Make sure employees know to call 911 when there is a threat of imminent danger.

MATURE your insider risk program over time by conducting self-assessments to determine the effectiveness of your deterrence, detection, and mitigation capabilities. Consider insider threat specific training for insider risk team personnel and coordinate with partners in your industry to identify best practices. Engage with federal agencies and organizations for access to resources.

INSIDER RISK AWARENESS

Insider Risk Job Aid



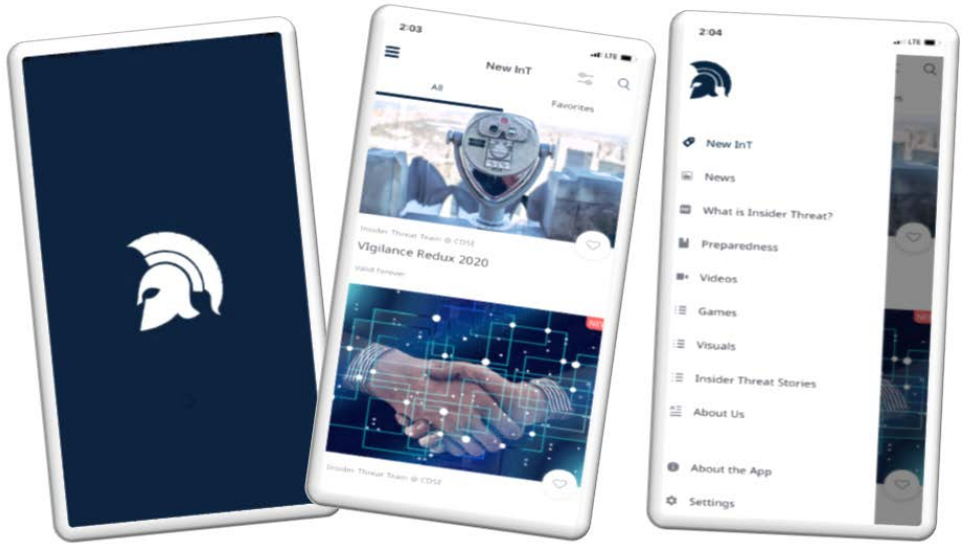
INSIDER RISK AWARENESS

AWARENESS MATERIALS AT WWW.CDSE.EDU

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

INSIDER RISK AWARENESS

Insider Threat Sentry - Mobile Application



GET IT ON Google Play

Download on the App Store

RESOURCES

DHS CISA
https://www.cisa.gov/insider-threat-mitigation

National Counterintelligence and Security Center/National Insider Threat Task Force
https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf

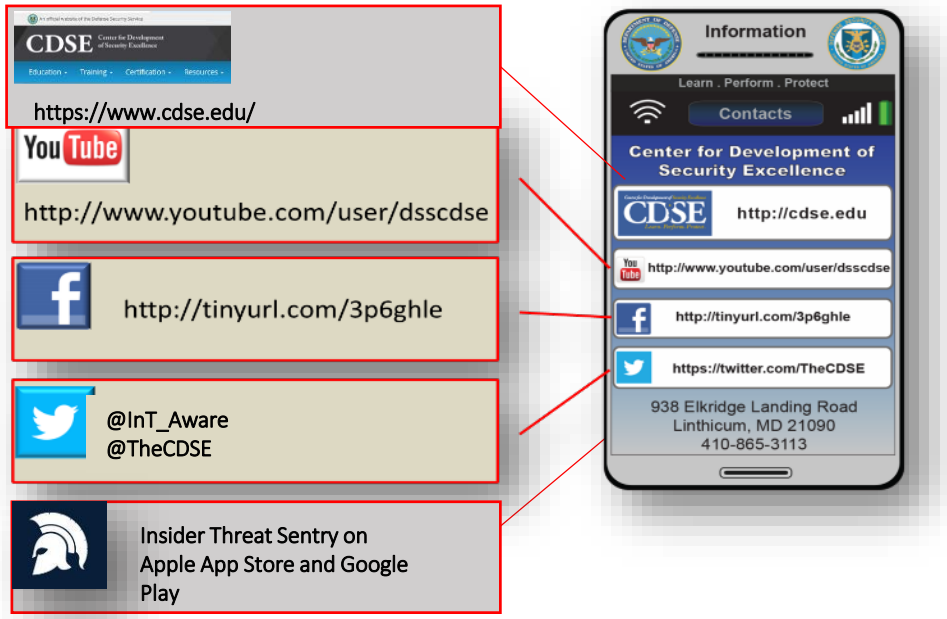
Defense Counterintelligence and Security Agency
https://www.dcsa.mil/

US Department of Agriculture
https://www.usda.gov/

Food and Drug Administration
https://www.fda.gov/home

FBI
https://www.fbi.gov/investigate/counterintelligence

WHERE TO FIND US



https://www.cdse.edu

Questions?

Rebecca Morgan
Insider Threat Division Chief, CDSE, DCSA
rebecca.a.morgan22.civ@mail.mil