DITMAC

NITAM NOTES

AUGUST 2025

SECURITY: PERSONNEL, PHYSICAL, AND INFORMATION SECURITY PARTNERSHIPS

COMPETING PRIORITIES

- Personnel Vetting (PV) utilizes information to make adjudication and access decisions, while InT uses similar data to assess concerning behavior and risk
- PHYSEC and PERSEC seek to stop access when risk behaviors are identified, whereas InT evaluations may require sustained access for further evaluation
- INFOSEC examines data/information loss to assess damage while InT uses that same data to determine who created the unauthorized disclosure and how

OPPORTUNITIES FOR COLLABORATION

- Share PV and InT information to help inform better adjudicative decisions, and improve data points for longer-term behavioral analysis
- Provide data on personnel who attempt to access unauthorized areas to support a more holistic insider risk picture
- Flag personnel with behaviors of concern for physical security and force protection to increase force protection postures
- Identify loss of proprietary, protected, or classified information early to help to reduce the suspect pool based on those with access, increasing odds of identifying the guilty actor

SECURITY CASE SUPPORT

- Share PV data, to include known personal predispositions, continuous vetting flags, and actions taken to date to inform InT assessment and management
- Understand physical and logical access by individuals who display behaviors of concerns and utilizing random antiterrorism measures and entry/exit inspections to help to mitigate potential risks
- Document previous information security incidents, like leaving classified information unsecured or bringing phones into unauthorized spaces, to inform risk assessment

BUILDING STRONGER PARTNERSHIPS

Mutual benefits to missions:

- The cross-functional integration of InT, IT, physical, and personnel security can be mutually advantageous to the overall success of their missions

Leverage developed standards:

- Recognize the well-established standards of each security program and understand their unique authorities and responsibilities

Share the ways InT can support security programs

- Identify individuals at increased risk by educating about concerning behaviors
- Make referrals to the security disciplines based on other information and data feeds
- Communicate to fill the critical gaps between security disciplines and other insider threat partners (i.e., CI, LE)

Highlight mutually beneficial relationships and shared interests:

- Increase value of security programs through shared information and common goals
- Ensure risk to individuals, information, and company/USG reputation are appropriately managed and mitigated
- Create efficiencies and potentially reduce demands on resourcing

KEY CONTRIBUTIONS

DETER

- Collaborate, sponsor, and support InT awareness through education programs
- Communicate available reporting options (e.g., DoD InT Reporting Portal)
- Remind employees of continuous vetting programs and the partnership with InT

DETECT

- Report anomalies and patterns of concerning behavior
- Share known incidents to determine if there is increased risk based on holistic review
- Provide background information on persons of concern to improve risk assessment

MITIGATE

- Take administrative action when necessary (i.e., report adverse clearance information, suspend access)
- Use entry/exit inspections and force protection measures (i.e., car sweeps, badge flags)
- Immediately report potential loss of critical info

DITMAC DOD Insider Threat Management and Analysis Center