PANEL DISCUSSION: OVER-THE-HORIZON AND EMERGING INSIDER THREATS

Wayne Belk

Co-Director

National Insider Threat Task Force

INSIDER THREAT MITIGATION

12 - 14 MARCH 2019

BRUSSELS BELGIUM

CO-HOSTED BY NNSA National Nuclear Security Administration FANC federal agency for nuclear control

insiderthreatmitigation.org

Insider Threat Minimum Standards by Category

INSIDER THREAT MITIGATION

Designation of Senior Official	
1 P	Designate a Senior Official
2 P	Create an Insider Threat Policy
3 P	Establish Implementation Plan and
	Produce an Annual Report
4	Coordinate program activities with proper authorities – OGC/CLPO
5 P	Create records handling and use procedures
6 P	Develop records retention guidelines
7	Conduct oversight reviews for policy & legal compliance

Insider Threat Personnel	
1	Program personnel trained in CI & Security fundamentals
2	Program personnel trained in conducting response actions
3	Program personnel trained in retaining, safeguarding and use of records/data
4	Program personnel trained in applicable civil liberty and privacy laws
5	Program personnel trained in applicable laws, regulations and policies and requirements – investigative referral requirements of Section 811

Access to Information	
1	Program receives timely relevant component information – CI & Security, IA and HR
2 P	Procedures to establish access to sensitive or protected information
3 P	Reporting guidelines for component departments to report relevant Insider information
4	Timely Access to CI reporting and Analytical products pertaining to adversarial threats

Monitor User Activity on Networks	
1*	Monitor user activity on all classified networks, either via internal or external agreements
	Conduct monitoring on at least one Classified network
2 P	Create policies for protecting, interpreting, storing and limiting access to user activity monitoring methods and results
3	Obtain signed agreements by all cleared employees
4	Ensure that there are classified and unclassified network banners informing users that networks are monitored

Information Integration, Analysis and Response	
1	Build and maintain an insider threat analytic and response capability – to ingest, review, centrally analyze, and respond to internal relevant information
2 P	Procedures for insider threat response actions – centrally managed by Insider Threat Program
3 P	Procedures for documenting each matter reported and response action taken.

Employee Training and Awareness	
1	Create procedures for initial & recurring training for employees to include documentation
2	Verify all cleared employees have completed required insider threat awareness training
3	Provide an internal network site to provide In Th information and to receive referrals

	Program Establishment
	Initial Operating Capability
	Full Operating Capability

P = Written guidance required

** Accounts for a tiered approach to achieving the minimum standards for monitoring users on classified networks*

CO-HOSTED BY National Nuclear Security Administration FANC federal agency for nuclear control

insiderthreatmitigation.org