Contribution ID: **534** Type: **Paper**

A New Approach to Insider Threat Mitigation: Lessons Learned from Counterintelligence Theory

According to the International Atomic Energy Agency's (IAEA) Information Circular (INFCIRC) 908, because "insiders possess access···authority and knowledge···[they] pose an elevated threat to nuclear security."Insiders, witting or unwitting, working together or alone, possess the opportunity to cause significant damage to nuclear facilities through sabotage or unauthorized removal of nuclear or radiological material. In response to this global threat, INFCIRC/908 pledged nearly 30 countries, with assistance from the IAEA and INTERPOL, to establish and implement a range of national-level measures to better mitigate insider threats at nuclear facilities. However, the relative lack of publicly available insider case studies involving nuclear facilities makes causal analysis and pattern recognition—which are necessary to better devise and propose effective protection/ mitigation efforts—difficult. Some insider threat researchers and practitioners have leveraged lessons from other disciplines to address this challenge. Prominent contributions to insider threat analysis include studies of high value jewelry heists and analyses of security measures within the casino and pharmaceutical industries.

One untapped discipline with key conceptual and practical similarities for eliciting insider threat mitigation insights is the field of counterintelligence. Counterintelligence, defined by United States Executive Order 12333 as "information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations,"provides a useful corollary to insider threat. Both counterintelligence and insider threat mitigation seek to protect high-value (or sensitive) assets from malicious, intentional human actions. Each discipline must contend with the challenge of identifying perpetrators from individuals with access rights that give them a privileged position compared to a traditional 'outsider'threat. In addition, the high security atmosphere of the Intelligence Community more closely approximates the uniquely protected environment of a nuclear facility than other civilian industries. Lastly, the consequences of failed counterintelligence and insider threat mitigation activities can both result in grave damage to national security.

This paper summarizes lessons learned from comparing conceptual similarities and empirical trends between counterintelligence activities and insider threat mitigation at nuclear facilities. After briefly reviewing insider threat lessons learned from other industries, this paper introduces the fundamentals of contemporary U.S. counterintelligence practice, including background investigations, mandatory reporting requirements, and the use of anomaly indicators for investigative purposes. Next, the paper outlines a comparison rubric and analytical framework for evaluating program goals, perpetrator characteristics, and protection efforts between counterintelligence and insider threat mitigation. Using U.S.-based counterintelligence case studies from the past several decades, this paper identifies key trends and insights across the motivations, characteristics, actions, and investigations applicable to insider threat mitigation. Lastly, this paper provides conclusions and lessons for potentially improving insider threat programs at nuclear facilities.

SAND2019-6133A Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525.

State

United States

Gender

Authors: WILLIAMS, Adam (Sandia National Laboratories); Mrs CAMP, Noelle (Sandia National Laboratories)

Presenter: WILLIAMS, Adam (Sandia National Laboratories)

Track Classification: PP: Insider threats