# Insider Analysis in the Secure Transport

# of Nuclear, Radiological, and other

# High-Risk Materials

Allyn Milojevich

Y-12 National Security Complex

Oak Ridge, Tennessee, USA

Email: allyn.milojevich@cns.doe.gov

Meghann Parrilla

Y-12 National Security Complex

Oak Ridge, Tennessee, USA

Abstract

Insider Quantification and Ranking Process (IQRP) is an assessment tool that effectively and accurately identifies and documents the potential negative effects an insider can have on a site’s protective posture. This analysis involves conducting interviews, physical protection analyses, and validating or invalidating current analysis documentation or assumptions. After completing the assessment, management can better determine the critical positions and consider ways to implement mitigation strategies, such as a Human Reliability Program (HRP).

## INTRoDUCTION

The Insider Quantification and Ranking Process (IQRP) is an assessment tool that effectively and accurately identifies and documents the potential negative effects an insider can have on a site’s protective posture. This analysis involves conducting interviews, physical protection analyses, and validating or invalidating current analysis documentation or assumptions. The "risk-based" interview questionnaire aids in the quantification, or scoring, of insiders based off individual access, authority, and knowledge, and uses a “defeat strategy” interview technique to capture the potential negative effects an insider can have on a facility’s protective posture. The scoring tool allows analysts to transition from qualitative information to quantitative data, similar to the Kepner-Tregoe process, to further prioritize the analysis results based on the criteria of significance. While individuals are interviewed and analysed, the interview questionnaire is designed to validate, or invalidate, assumptions associated with *job categories* and associated capabilities. Capabilities include access, authority, and knowledge. Questions on access and authority tend to be closed-ended (black and white), while knowledge robustness questions are more open-ended (grey). After the questionnaire is complete, answers are scored based on a ranking matrix.

To be clear, this tool is designed to assess positions, in particular the potential for individuals in different positions to become inside threats, and how dangerous an insider threat they pose based on their position. It does **not** identify individuals that are nefarious insiders or have the potential to become nefarious insiders. After completing the assessment, management can better determine the critical positions and consider ways to implement mitigation strategies, such as a Human Reliability Program (HRP). Until now, this process has mostly been tested and implemented at static sites for site specific physical security. This paper will discuss its application to secure transport, including adaption and potential adoption by secure transport operators.

The major benefit of the IQRP is that it is an assessment tool that requires minimal costs aside from staff time, unlike implementation of an HRP, which requires capital investments. Background screenings, periodic monitoring, and continuing medical examinations through an HRP require major investments. The IQRP will better aid in the development and implementation of a cost-effective and efficient personnel security or HRP by better identifying positions that would be subject to an HRP. The IQRP simply requires the time of several staff members. It is an enlightening evaluation in that management often does not see the way that insider potential varies from individual to individual and from position to position. This assessment tool provides quantitative data that facility management can use when considering how to address the concerns over insider threat. These benefits make it especially beneficial in the international community, which may not have the resources to invest in large-scale HRP or other insider mitigation programs.

Nuclear and radiological material is most vulnerable when it is being transported, which makes the identification of critical positions during transport all the more important. The relationship between facility staff (at both the shipping and receiving locations), contractors, and responders, including local law enforcement, requires additional screenings and identification of trustworthy personnel throughout the transportation process. This paper will describe the process and highlight how IQRP can be applied to secure transport, especially when considering the role of contractors, coordination between the transporter and local law enforcement, and the role of response to a potential incident.

## INSIDER QUANTIFICATION AND RANKING PROCESS

## IDENTIFY INSIDER JOB CATEGORIES

The first step of the IQRP is to identify and prioritize insider job categories that potential pose a risk to the security of nuclear transport. In order to accurately identify the job categories, analysts must have an understanding of the current configuration of the facilities, including physical security measures and facility specific job duties and responsibilities related to shipping and receiving, knowledge of the physical protection posture during shipping, and understanding of the detection and response to a security incident. The following process is used to identify job categories to be interviewed:

The analyst should use facility records to identify job categories that have authorized access to the asset, which are the most important job categories for assessment. This includes positions with authorized hands-on access to the asset, systems that control the asset, or systems that control the security of the asset. In addition to job categories that have access to the asset, job categories that have authority over those who have direct access to the asset should be analysed. Authority can include supervisory positions and response force. Lastly, any other job categories that have access to the area should be identified, including escorted access.

Analysts should differentiate between direct and indirect access to the asset. Direct access is defined as job categories who have authorized access to place hands on the asset or systems that control the asset. Indirect access is defined as job categories who do not have authorized access to place hands on the asset or systems that control the asset but have access to either storage or processing areas (i.e. proximity to the asset). Job categories that meet the above criteria should be interviewed and ranked to determine potential insider risk.

## INTERVIEW PROCESS

The interview questionnaire is designed to validate, or invalidate, assumptions associated with job categories and associated capabilities. Insider capabilities include access, authority, and knowledge. Questions for access and authority tend to be closed-ended while knowledge questions are more open-ended. The following steps are used in the Insider Interview Methodology.

### INTERVIEW

Simply talking with employees ensures an understanding of the actual employees’ attributes and can validate any remaining assumptions. Analysts should use a specific Insider Interview Questionnaire to ensure consistency throughout the Insider Analysis. Questions used in the interview should be focused on gaining information specific to insider objectives. The Insider Interview Questionnaire is segregated into four topic areas: General Information, Access Capabilities, Authority Capabilities, and Knowledge Capabilities. General Information captures general information about the specific person being interviewed, such as job title, job description, years of service, years in current role, previous jobs/positions, clearance level, and two-person rule certified. Access capabilities capture the employee’s access capabilities to material, facilities, procedures and systems. Authority captures the employee’s capabilities within systems, administrative procedures, and other employees. Knowledge is the most complex attribute to analyse. Insider knowledge is comprised of knowledge of the asset itself, the facility, and protection measures.

#### Setting up the Interview

Prior to the interview, the analyst should obtain maps, blueprints, or any other documents necessary for reference during the interview.

#### Interview Process

Using the Insider Interview Questionnaire, the analyst will document the information obtained from the employee. Access and authority questions are close ended, which usually can be answered with a simple “yes” or “no.” Access and authority are attributes that the employee either has or does not. Knowledge questions are open-ended and require more thought than a simple one-word answers.

General Information

While the IQRP is designed to assess categories of jobs and their relation to potential insider threat, it is also important to understand the individual employees within the job categories. It is important to obtain and document general information, such as the employees previous job duties, years of service, facilities that employee works in (if necessary), and any programs the employee may be in, such as HRP. The IQRP quantifies the average employee’s access, authority, and knowledge within each job category. Previous job positions have their own set of attributes different than current attributes, and the knowledge gained from that experience is not forgotten. It is particularly important to analyse the employees perceived job duties versus actual documented job duties. In many cases, employees take on more responsibilities and duties than what is expected or written. This can reinforce their perceived need for access and authority.

Access Information

Access considers authorized access to facilities and programs, to include personnel, information, equipment, and system. An insider presents a unique challenge to the physical protection system as insiders can use defeat methods not available to outsiders to bypass protection measures and access control procedures. Analysts should pay particular attention to direct versus indirect access, escorted versus unescorted access, and cyber access. Importance of access is specific to the transportation process at hand, including whether the access is at the shipping or receiving facility, as compared to access to the nuclear material on the vehicle during transit. The following represents a sample of access questions to ask:



Authority Information

Authority considers the employees authority over personnel, systems, and equipment. Systems to consider are security systems, such as alarm systems, badging systems, and Nuclear Material and Control tracking systems. Additionally, the analyst should pay particular attention to personnel who have authority to assess, conduct maintenance, or performance test on alarms. The following represents a sample of authority questions to ask:



Knowledge

To capture the knowledge of an employee, the analyst uses a “defeat strategy” type of interview. Using the defeat strategy interview methodology, the analyst can gain a holistic understanding of the employee’s knowledge, including asset and facility information, as well as any protection measures and weaknesses associated with those methods. This type of technique enables the employee to recall information based on daily interaction and facility access. The defeat strategy interview technique is conducive to a more comprehensive analysis of malicious acts that could be committed by an insider within their current job roles.

The defeat strategy interview technique must be adjusted based on the job category and the information the analyst is trying to receive. Typically, the defeat strategy interview technique incorporates the following topics at high level:

* Asset
* Locations, attributes, protection measures, etc.
* Facility
* Protection measures to includes access controls, alarm systems, response force, etc.
* Building Construction
* Ingress/Egress routes
* Emergency evacuation procedure
* Transportation
* Protection measures
* Construction
* Transportation routes

The employee’s answers to the above questions determine the interview path forward. The analyst may choose to ask more questions on the various sub-topics to gain a better understanding of any potential malicious activity that could be caused by an insider. The ultimate goal of the interview is to assess the totality of access, authority, and knowledge that an individual holding a job has. Once multiple individuals are interviewed within a job category, assessments can be completed to determine how critical different positions are to a robust transportation security system.

## RANKING INSIDER ATTRIBUTES

Upon completion of the interview, the analysts should use a ranking criterion to transition the qualitative information obtained during the interview to quantitative results. Ranking criteria should be dependent on the site; however, a simple approach is to rank employees’ attributes as HIGH, MEDIUM, LOW based on the interview answers.

The following table is an example of ranking criteria for access attributes:



The following table is an example of ranking criteria for authority attributes:



The knowledge attribute ranking can be categorized by the following:

* Low: Information gained from the public domain. Examples include the internet, library, blogs, newspapers, social media, etc. It is usually assumed that all types of insiders have this level of information.
* Medium: Information gained from having physical access to an area. This allows insiders to gain information that is readily available, but not specific or restricted to a particular job duty.
* High: The most detailed level of knowledge and is usually associated with a particular job function.

As stated above, the results of the employee interviews for each job category should be averaged to ensure an accurate representation of the job categories access, authority, and knowledge attributes. The following tables provide a representative example of results of access, authority, and knowledge, respectively.







It is important to analyse the job categories attributes both individually and holistically. To analyse the potential risk of an insider acting alone, particular focus on the worse case insiders for the access attribute should be considered. To analyse the potential risk of an insider colluding with an adversary force, a holistic focus on the worse case insider for the knowledge, access, and authority should be considered. Additionally, the results should influence job categories that require mitigation as well as inform potential mitigation programs.

## INSIDER MITIGATION

Insider Threat Mitigation Programs (ITMP) are often costly and labour intensive to implement and tend to be extremely distinctive for individual sites. The rigor and level of the ITMP is typically based on the asset, security and organizational culture, and finances. Additionally, mitigation programs vary to include physical security systems, administrative controls, and comprehensive programs. Physical security systems are comprised of intrusion detection, access controls for both prohibited and controlled articles and locks, barriers, etc. These type of mitigation programs potentially prevent insider job categories that do not have authorized access and/or preclude nefarious insiders. Administrative controls could include Tamper Indicating Devices, Daily Administrative Checks, Inventories, Material Transfers, etc. Although, this type of mitigation program does not typically provide immediate detection, it potentially deters insiders with authorized access. Lastly, comprehensive programs could encompass a Two Person Rule, Human Reliability Program (or trustworthiness), clearance investigations, cyber, Incident of Security Concern, Local Insider Threat Working Groups, etc.

Data gathered from insider interviews should be used to inform risk-based decisions regarding insider mitigation. To ensure a proper level of an ITMP is implemented, an assessment of the insider risk should be conducted to understand the risk and cost benefit. Resources may not be available to invest in large-scale HRP or other insider mitigation programs; therefore, it is imperative the appropriate level of mitigation programs is implemented to maximize cost savings. It is imperative to understand the advantages and disadvantages of the various ITMPs when determining the rigor of mitigation programs. The more attractive the asset, most likely, a higher level of ITMP should be implemented; however, culture may not allow essential programs. With a proper insider threat analysis, the most cost effective and advantageous ITMP can be determined.

For transportation security, it is vital to assess job categories across the entire transportation process, from packaging and shipping from the first facility, contractors or staff involved in packing the asset on to the vehicle, individuals responsible for monitoring vehicle movements, and responders involved in the shipment planning as well as response to a potential incident. It is important to interview a representative sample from each stage of the transportation process to determine which position are most critical for inclusion in to a formal ITMP, such as an HRP.