Vulnerable Position Identification

Patrick Lynch
Lawrence Livermore National Laboratory

Abstract: In 2020, a multi-discipline team sponsored by the U. S. Department of Energy's National Nuclear Security Administration (DOE/NNSA) Office of International Nuclear Security, evaluated key positions associated with the transportation of nuclear material. These positions were assessed based on the individual's access, authority and knowledge, the three key elements of an insider. An elementary methodology was developed for this process and each position was assigned a color-coded determination, green, yellow, and red. Red indicated the position with the most cause for concern for exploitation. This assessment has initiated a discussion to explore similar rankings of vulnerable positions, allowing for a tailored mitigation method to be created based on the most vulnerable, by access, authorization, and knowledge, to be developed at nuclear fixed sites. This paper and presentation is meant to define the potential for applying this elementary methodology to fixed sites and ascertain the applicability of this process among the global nuclear community.

Introduction

Insider threats within the nuclear industry pose special challenges to operational safety and security. This paper will include definitions of insider threats from across the global community. These definitions vary slightly, which will influence the discussion section of this paper regarding potential next steps in implementing mitigation strategies for the, potentially, most vulnerable positions. The use of nuclear industry is also quite vague as this industry contains many elements to which staff with access, authority and knowledge could be an insider threat. The transportation of nuclear materials poses unique risks as it increases the variables, opportunities, and vulnerabilities a nefarious actor can exploit (Transportation Factsheet, 2020). In addition to these vulnerabilities, insider threats within the transportation of nuclear materials increase the potential risks, which is one reason this initial assessment of vulnerable positions was conducted. This paper will also include some requirements of the Nuclear Regulatory Commission (NRC) in the United States addressing the commercial nuclear sector. These requirements include specific designations of those employees which are placed in Critical Groups, identified with broad unescorted access, positions of authority, and staff with intimate knowledge of some of the most critical elements of the facility's operations (US NRC, 2008). Finally, this paper will also include descriptions of trustworthiness and reliability elements that may be considered when identifying these positions most vulnerable, or susceptible, to insider exploitation.

It is also important to note that this evaluation is solely focused on the positions, not the individual or the tasks. This is an important distinction. Other research may focus on an individual, their behaviors, attitudes and, possibly, character. These traits are some of what the basis of an Access Authorization or Fitness-for-Duty program would be built upon. Ensuring the trust determination in an individual is made prior to that individual receiving access, authority, or knowledge. There are ongoing evaluations to ensure that these individuals are within programs such as Behavioral Observation or continuous monitoring, to maintain the highest levels of trustworthiness and reliability. In addition to the positions and tine individuals, a follow-on project of value may be to evaluate the tasks required at the site during operations. The tasks

themselves may provide to provide unique insider risk concerns if an individual can exploit elements of a task to accomplish their insider goals. A job task analysis is a common practice within Human Resources to determine the knowledge, skills, and attributes best suited for a position. However, there may not be research on task analysis from an insider vulnerability perspective, future research areas will be included at the end of this paper.

Definitions

The United States Department of Defense and the United States Department of Energy define Insider Threats and have mitigation measures commensurate to the levels of harm insiders may create based on their access, authority and knowledge. For the purpose of this paper and the intent for its application broadly across the global nuclear community, definitions will be taken from the international community and the United States Regulatory Commission in the context of operating nuclear power plants. The International Atomic Energy Agency (IAEA) defines an insider threat as:

> *"an individual with authorized access to [nuclear material,] associated facilities or associated activities or to sensitive information or sensitive information assets, who could commit, or facilitate the commission of criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities or associated activities or other acts determined by the State to have an adverse impact on nuclear security" (IAEA NSS8-G,2020)*

The World Institute for Nuclear Security (WINS), which is an international non-governmental member organization that strives to be a leader in knowledge exchange, professional development and certification for nuclear security management. WINS defines an insider as:

> *"Insiders are individuals who may take advantage of their authorised access to facilities, processes, materials, transport operations or sensitive computer and communications systems to perform a malicious act." (WINS IBPG, 2015)*

To complement the US Department of Energy and Department of Defense definitions, the U.S. Nuclear Regulatory Commission (NRC), which regulates government and civilian nuclear infrastructure defines an insider as:

> *"A trusted person with protected or vital area access, or access to digital computer and communications systems and networks from outside the protected area, can pose a significant threat to the safety and security of a nuclear power plant…" (US NRC, 2008)*

The common themes throughout these definitions include the ability of an individual to leverage his/her access within a nuclear facility, or information. Additionally, the other two key themes include authority and knowledge, which are synonymous with successful, and unsuccessful, insider actions throughout history. Access, authority, and knowledge will be the basis of the evaluation of the positions throughout this paper, considering the vulnerable positions in both the transportation of nuclear materials as well as at fixed sites.

Transportation Security Examples

As an adversary, either external or internal, seeks to exploit access, authority, or knowledge, their task can be much easier when a target, such as nuclear material, is in transit. Roles that can be exploited span the entire transportation process. While there are numerous possible roles to exploit, there are less positions that have high potential for threat in terms of the most important factors of access, authority, and knowledge. These positions may require greater preventative measures to reduce risks, which can include more stringent background investigations, more frequent reinvestigations, financial and criminal evaluations, and drug/alcohol testing programs. To best address the varying positions that encompass materials as they are transported from one site to another, an interdisciplinary team broke this down into three phases, the initiation phase, the transport phase, and the destination and support phase, see Table 1 for the list of the identified positions.

Table 1

Identified General Positions based on the Initiation phase, Transport Phase, and the Destination Phase

Initiation Phase	Transport Phase	Destination Phase
Site Operations/Facility Staff	Sea Vessel: Captain	Security Force/Officers
Facility Management	Crew	Commanders
Facility Regulators	Owner	Dispatch
Site Security Management	Flag Regulator	Support Staff
Site Support Staff	Maritime Organization	Other Organizations: Government
Temporary Contractors	Rail: Engineer	Conveyance Tracking Organization
Package Operators	Rail Dispatch	Regional Entities (Euratom)
Package Owner/Management	Rail Company Management	Government Authorities
Support Staff	Maintenance Personnel	Site Operator/Facility Staff
Transport Coordinator	Asset Tracking Center	Facility Management
Freight Forwarder	Truck Driver	Facility Regulators
Transport Coordinator Management	Road Dispatch	Site Security Management
Government Coordinator	Trucking Company and Management	Site Security Operators/Guards
	Asset Tracking Center (Road)	Site Support Staff
	Port Authority/Operator	
	Port Workers	
	Port Security/Access Control	
	Customs and Maritime Authority	
	Naval/Military and Vessel Agents	

Note. These positions were taken from the Transportation Security Factsheet, 2020. Additional analysis on each position is available within the factsheet.

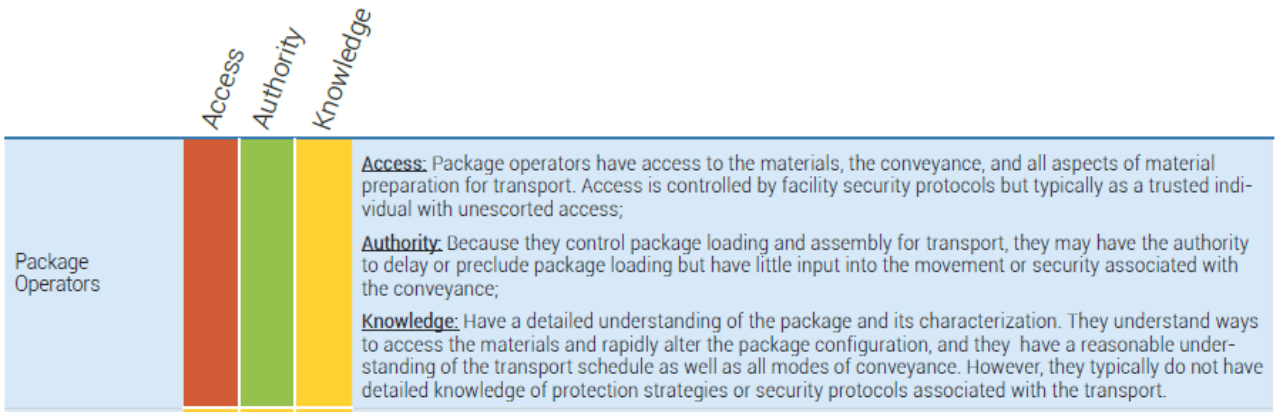
An elementary methodology was developed, leveraging transportation and insider threat expert knowledge and familiarity. The methodology included a survey among these experts evaluating each position and assigning a numerical value, with 10 being high levels of access, knowledge, and authority, and 0 being little to no access, authority, or knowledge. The team then assigned a color (red, yellow, green) based on the numerical value assigned to each position, see Table 2. The assignment of colors is also a generalization based on the experiences of a largely U.S. team of experts and is not meant to reflect the potential vulnerability of positions at each facility globally.

Table 2
Color Based Assignment of Security Threat Potential

	High Security Threat Potential
	Medium Security Threat Potential
	Low Security Threat Potential

Note. These rankings were taken from the Transportation Security Factsheet, 2020. Additional analysis on each position is available within the factsheet.

Figure 1
Example Evaluation for Package Operators based on the Assessment.



Note. This Figure is derived from the Transportation Security Factsheet, 2020. Additional analysis on each position is available within the factsheet.

Above, in Figure 1, is an example of the initial analysis of one position, Package Operators and the reasoning behind why the position was rated this way. For a Package Operator, they are known to have access to the materials, the conveyance and all aspects of material preparation for transport. Additionally, access is controlled by facility security protocols but typically as a trusted individual with unescorted access. A Package Operator has limited authority in the control of materials, loading and assembly for transport. They may have the authority to delay or preclude package loading but have little input into the movement or security associated with the conveyance. Finally, the knowledge that a Package Operator has is rated a medium due to their detailed understanding of the package and its characterization. They likely understand

ways to access the materials and alter the configuration, while also having an understanding of the transport schedules and modes of movement. This position typically does not have detailed knowledge of protection strategies or security protocols associated with the package movement.

Critical Group within Fixed Sites

The Transportation Security Factsheet (2020) has a similar analysis of all forty-six positions identified by the multidisciplinary team. Each of these positions may have varying levels of trustworthiness and reliability measures applied to each position. The NRC regulatory requirements, 10 CFR part 73 describes physical protection of nuclear power plants and materials. In this requirement, elements of the Insider Mitigation Program (IMP) are outlined, which has led to the Nuclear Energy Institute's Access Authorization and Fitness-for-duty documents which are resources to the nuclear power plant licensees as they implement the required IMP measures. In an effort to enhance the existing regulatory requirement, in 2008 the NRC published Regulatory Guide 5.77 which strengthened the IMP and identified a "Critical Group" of employees who were assessed to be most deserving of access, authority and knowledge across a facility. The Regulatory Guide identifies the following criteria to be determined among the fixed sites:

- "*any individual who performs job functions that are critical to the safe and security operation of the licensee's facility;*
- *Any individuals who have extensive knowledge of facility defensive strategies or who design and/or implement the plant's defense strategies;*
- *any individuals in a position to grant an individual unescorted access or to certify an individual unescorted access authorization;*
- *any individuals assigned a duty to search for contraband (e.g., weapons, explosives, incendiary devices);*
- *any individuals who have access, extensive knowledge, or administrative control over plant digital computer and communication systems and networks as identified in § 73.54; and e. any individual identified in 10 CFR 73.56(i)(!)(v)(B)(5)"* (NRC, 2008, pages 14-15)

These position descriptions describe the levels of access, authority, and knowledge, which is determined by the plant, or licensee, and then reported back to the NRC. The document and indicates that there area some preventative measures that are applied to these positions, for example there is a 3 year background investigation instead of a 5 year reoccurrence. There is also likely more stringent reviews and assessments of individuals being hired into a Critical Group position. If an Insider Threat Mitigation program is developed for the international community that is dedicated to positions, a set of trustworthiness and reliability measures will need to be developed, in a graded approach, to align with these Critical Group roles. This is likely to be unique to a facility, the site's security posture, the nation's legal and regulatory framework, as well as the types of threats posed to the site and its staff. It will also need to be determined what, if any, adjustments may be required if this this assessment is applied to an existing facility. For example, if the Transportation Security Factsheet approach is used for a mature site.

Next Steps

Evaluating the individual is one of the common Insider Threat Mitigation practices, but this approach to assessing the positions may allow for a more thorough program evaluation. The Transportation Security Factsheet is comprehensive and, based on subject matter input, has identified some positions that may be vulnerable to insider exploitation if the wrong person has the position. To apply this methodology to a fixed site, leveraging the requirements from the NRC, as described in the Critical Group designation, a team will need to assess the levels of access, authority and knowledge across a facility. This may then determine if varying levels of trustworthiness and reliability measures need to be increased based on the position. To determine this, questionnaires and interviews will need to be conducted, applying a numeric value to the levels of access, authority and knowledge for each position. Following the assessments, a determination of ranking may occur, which may point to the positions which have the greatest access, authority and knowledge. A corresponding trustworthiness and reliability program can be compared to evaluate any gaps or potential for individuals to gain positions that are of highest consequence. As mentioned earlier, a graded approach based on the country's, company's and site's culture, legal and regulatory framework, as well as threat may be developed.

To include another aspect of a mitigation program, it is recommended that a team also evaluate the task which are completed at a fixed site. It is possibly that an individual is trustworthy, they are in a position that does not provide too great of access, authority or knowledge, but their tasks performed actually can either create an unwitting insider action or can be exploited by an insider with knowledge of the tasks. Much like the evaluation of positions, the task evaluations may also be sensitive and it will be important that any specific information on the individuals, positions, or tasks is managed with high levels of attention.

Acknowledgments

Much of the topics, themes, and examples discussed in this short proposal paper and accompanying presentation are possibly due to the direction, funding, and oversight of the DOE/NNSA Office of International Nuclear Security. The Office of International Nuclear Security has a number of technical teams, one of the teams, the Transportation Security Functional Team worked to develop the Factsheet.

LLNL-PRES-849264

References

Nuclear Regulatory Commission (NRC). *Regulatory Guide 5.77.* Office of Nuclear Regulatory Research, Washington D.C., 2008

IAEA, *Preventive and Protective Measures against Insider Threats*, IAEA Nuclear Security Series No. 8-G (Rev. 1), IAEA, Vienna, 2020.

Transportation Security Factsheet, Developed by the Office of International Nuclear Security, 2020.

WINS, International Best Practice Guide, *Managing Internal Threats. V. 2.1,* 2015