Proceedings of the International Symposium on the Packaging and Transportation of Radioactive Materials
PATRAM 2019
August 4-9, 2019, New Orleans, LA

Offsite Source Recovery Program Insider Threat Analysis*

Ken Martin, Program Manager
Oak Ridge National Laboratory
Oak Ridge, TN 37831

Commie Byrum
Oak Ridge National Laboratory
Oak Ridge, TN 37831

Shannon Morgan
Oak Ridge National Laboratory
Oak Ridge, TN 37831

ABSTRACT

The transportation of radiological materials plays a critical role in medical, industrial, and commercial applications. Insider threat is a concern to the radiological transport industry because of an insider's ability to bypass or defeat multiple and dedicated elements of a security system with their access, authorities, and knowledge. This paper recommends methodologies to help mitigate the potential insider threat by improving technical capability and reducing the risks associated with the malicious use of radiological materials.

1. INTRODUCTION

The insider threat poses one of the greatest risk management challenges to personnel and organizations in both the Unites States and abroad. The radiological transportation sector is not immune to this risk. The growing impact of insider threats poses security risks to private sector companies as well as to the national and economic security of the United States (Rose, 2016). If an attack were to happen, it would not only affect the commercial industry but also the entire United States. As stated by the U.S. Chamber of Commerce, "American business has a multifaceted stake in a strong national defense and a homeland security policy that safeguards Americans while also protecting their mobility, their freedom and their way of life" (U.S. Chamber of Commerce, 2010).

An attack targeting radiological material is of concern because of the widespread use of radioactive material in several sectors including medical, industrial, and academic settings. A successful attack on a radiological shipment could lead to the loss of a risk-significant amount of radiological material that could be used by the adversary in a radiological dispersion device (RDD) or radiological exposure device (RED) (U.S. NRC, 2014). Studies have shown that an RDD attack would be unlikely to produce enough radioactive contamination to kill or injure anyone. The only direct medical effect from such an attack would be an increased long-term cancer risk, but several complications would follow such an attack. However, one chief issue is that if an RDD were used in a major municipality, the economic losses could be in the billions or even tens of billions of dollars (Jones, 2016). Added to this loss would be the psychological impact to the population and the potential loss of confidence in the government both domestically and internationally. Furthermore, the psychological impact of an RDD would be nearly the same as one employing a nuclear weapon. Whereas the fallout from a nuclear weapon cannot be replicated with an RDD, the negative association of radiation and its effects would be present. Fear, anxiety, and a demand for medical services by both those exposed and those who fear exposure would cause major problems for medical

facilities. Medical providers would be quickly overwhelmed by this demand for services. The demand for medical and psychiatric services would continue for months, if not years, after such an attack (McBride, 2008). For these reasons, it is critical that radioactive sources be secured both at fixed sites and while in transport. An especially important aspect to consider is that these materials are most vulnerable while being transported. A major step to ensuring the security of these sources is the mitigation of the insider.

This paper presents the results of the analyses of the insider threats specific to the Off-Site Source Recovery Program (OSRP), which is a program within the National Nuclear Security Administration. The OSRP recovers excess, backlogged, orphaned, or unwanted sources from facilities across the United States (Los Alamos National Laboratory, 2018). A qualitative analytical insider model was developed that provided a simple and effective means of simulating the conduct of an adversary. This analysis developed a framework to model the insider and then performed an analysis of the insider in relation to the transportation of radiological materials. The analysis recommended several actions to assist in building an effective security program to mitigate the insider threat, including background checks, continuous monitoring, enhanced physical security systems, and training. In addition, it is important to understand that every individual who has physical or remote access to the material during transit has the potential to do serious harm. Almost every incident of theft involving nuclear materials in which the details of the incident are known was committed by an insider or by outsiders assisted by an insider accomplice (Bunn & Sagan, 2014).

2. OBSERVATIONS

The objective of the OSRP study was to evaluate the risk the insider threat poses specifically to the radiological transportation industry. Additionally, the assessment was conducted to identify deficiencies within the operations of the OSRP recovery process that could impact the overall security of the organizations, personnel within the industry, and the public. Furthermore, the study was intended to develop recommendations for improvements that would inform decisions makers for resource allocation to reduce those risk and enhance organizational resilience through countermeasures and mitigation strategies.

The security features that are provided for the radiological shipments are intended to restrict unauthorized access to the radiological sources; however, many of the security features were designed prior to the concern about RDDs. These features provide a minimum amount of protection and safety features, but they may not be entirely effective against a determined and knowledgeable adversary, especially an adversary profile described in the ORS Potential Adversary Capabilities list (Gitomer, O'Brien, Mason, Strub, & Van Tuyle, 2003). Nevertheless, anything that deters one from removing a source can provide a measure of protection and reduce concern, but there are areas for improvement. To address these concerns, a mixture of enhanced administrative and physical controls should be implemented.

There were four areas that were identified during the OSRP study that present an opportunity for improvement. By focusing on these four areas, the OSRP team(s) and the commercial industry can make significant progress in ensuring the secure transportation of radiological material. The following four areas are discussed:

- Trustworthiness Program
- Insider Threat Mitigation Program
- Information Security
- Physical Security Systems

2.1 TRUSTWORTHINESS PROGRAM

The cornerstone of any security program is ensuring that only trustworthy and reliable people have access to critical information, systems, and assets. Without this essential element in place, other security measures are much less effective. Background checks are required for some positions that have unescorted access to Category 1 and 2 radiological material, but there is room to enhance the processes that are in place regarding the personnel security aspects of the radiological transportation program. 10 CFR 37.21 requires a personal history disclosure, a criminal history records check, and fingerprinting for personnel who have unescorted access to Category 1 & 2 radiological material, but there are several personnel/positions that are exceptions to this requirement. These entities who are exceptions to 10 CFR 37.21 have access to the conveyances and/or information concerning the shipment and include personnel at the state or local government level (i.e., law enforcement) and others.

Though some individuals receive a background check, the information gained from the background check is not required to be compared with other data such as credit checks, civil court activity, foreign travel, driving history, or social media. One of the limitations of only performing a criminal records check is that it may not detect if a person has an alcohol or drug problem, which would pose a concern in determining whether he/she is trustworthy and reliable, whereas an in-depth review that included interviews of the personnel's contacts would. Also, a criminal records check will not let the employer know the individual's financial status. Title 32 Part 147 – Adjudicative Guidelines for Determining Eligibility for Access to Classified Information states that "f*ailure or inability to live within one's means, satisfy debts, and meet financial obligations may indicate poor self-control, lack of judgment, or unwillingness to abide by rules and regulations, all of which can raise questions about an individual's reliability, trustworthiness, and ability to protect classified information"* (United States Government, 2012). While the information concerning these shipments is not classified, it is very sensitive and needs to be protected by people who are trustworthy. The absence of these additional checks does not allow management or the reviewers for trustworthiness and reliability to build an overall risk profile for these individuals. Because of the danger these materials present, there is a compelling public interest in requiring this information to be evaluated in its entirety to assess the trustworthiness and reliability of personnel with access and knowledge regarding this material.

As stated earlier, some personnel are exempt from the requirements in 10 CFR 37.21, and commercial drivers fall into this category. However, drivers are subject to 49 CFR 1572, which does require them to be subject to a security threat assessment process conducted by the Transportation Security Administration (TSA) every 5 years to receive a Hazardous Materials or HAZMAT endorsement, but one could argue that the disqualifying criteria are lacking. The requirements for this endorsement are a security threat assessment that includes fingerprinting by the state or the TSA along with a search within the FBI/Criminal Justice Information Services database and a search of the following databases.

Interpol and other international databases

- Terrorist watchlists and related databases
- Any other databases relevant to determining whether an applicant poses, or is suspected of posing, a security threat, or that confirm an applicant's identity

If there is no disqualifying information found after the review of the applicant's application, the endorsement is issued for the transportation of hazardous material. Analysis has shown that the driver is most likely the number one threat when it comes to the insider. This lack of a comprehensive background check is troubling and should be addressed.

Also, for organizations that would like to complete a more thorough investigation, there are obstacles they must overcome. There is no unified database for the organizations to access to conduct background checks, so they must search within state, county, and municipality records. Also, criminal records are sealed in some states, and laws vary according to when these are sealed. This leaves the organizations in a situation where they may not have a complete profile of the individual (Brody & Cox, 2015). Finally, mental health records cannot be accessed in some states, and the federal government does not make medical records available to its National Instant Criminal Background Check System (Timmins, 2013).

The OSRP primarily uses a mixture of cleared drivers and material recovery personnel who go through a much more thorough background check than other personnel who simply have a background check for trustworthiness and reliability or those who possess a HAZMAT endorsement. However, it should be noted that all OSRP drivers do have a background check in addition to the HAZMAT endorsement, but it is not necessarily equivalent to a security clearance background check. This lower standard of investigation creates the risk of allowing unreliable personnel to have access and knowledge of the information and assets that are being protected. Checks for trustworthiness are only required to be reinvestigated every 10 years, which is another area for improvement. A background check only represents a moment in time, and the information may change as time goes on. Therefore, more frequent reinvestigations should be established.

The use of cleared personnel should be considered a good practice, but it is important to understand that an effective insider mitigation program should be executed along with the background/clearance process. The implementation of a continuous evaluation process would allow for a proactive, accurate, and actionable assessment of risk-causing events within the program. Continuous warning of such events would allow organizations to shift from reactive responses to proactive mitigations (Izurieta, 2018).

2.2 INSIDER THREAT MITIGATION PROGRAM

The security protocols that currently exist within the radiological transportation industry do not properly address the insider threat. During the analysis, the team did not find any indication that the industry has any program to address the insider threat. Because of the ability of the insider to seriously degrade system effectiveness, an insider threat program is needed to assist in ensuring the safe and secure transportation of radiological sources. The program should be implemented through the policies and procedures of the organizations within the industry. The program should build upon the trustworthiness program that is in place by implementing some type of continuous monitoring program of personnel. As stated earlier, an individual's circumstances, attitudes, behaviors and motivations will change over time, so some type of continuous monitoring program is critical. Even if an employee may not have had any negative information in his or her background at the time of employment, a stressful life event such as a DUI, bankruptcy, divorce, or other significant event can change a person's risk profile in an instant (Ananthanpillai, 2015). This program would help to ensure operational and security reliability and bolster the current security features. There are no indicators that the industry currently conducts training related to insider threats. Without a policy and training to address the insider threat, organizations may not have the tools to recognize the indicators of an insider threat, be aware that this threat exists, or know how to respond and mitigate the threat. One of the most critical areas regarding insiders is the papering of a potential threat. In most past cases, relevant information was available yet went unreported (Sandia National Laboratories, 2015). It is imperative that individuals know that they need to report any suspicious behavior, and they need to know how to report the incidents.

2.3 INFORMATION SECURITY

The lack of information security within this program is a concern. 10 CFR 37.43 requires that "licensees authorized to possess category 1 or category 2 quantities of radioactive material shall limit access to and unauthorized disclosure of their security plan, implementing procedures, and the list of individuals that have been approved for

unescorted access." However, due to the need to complete these shipments, information regarding these shipments is broadly distributed. Notifications are sent to many different entities regarding the details of these shipments. What cannot be determined is how this information is protected once it has been communicated or if it is protected. However, all the requirements concerning information security fall primarily on the licensee. What is not specified in the CFR is how the information is to be protected once it is at the state level. One example of this issue is the notification to law enforcement escorts 2 weeks prior to a shipment date. This advanced knowledge coupled with the lack of a trustworthiness program has the potential to create a vulnerability. In addition, this information is sometimes distributed by email to law enforcement, which is password protected, but there are numerous examples of hackers defeating passwords. As one writer wrote in an industry website, "nothing you do, no precaution you take, no long or random string of characters can stop a truly dedicated and devious individual from cracking your account" (Hill, 2012).

Another example of the lack of information security was observed on a recovery. During one of the recoveries, the Oak Ridge team observing the process overheard a staff member from the licensee facility ask a member of the source recovery team where the source was going. He very loudly replied, "We are sending this to Texas." Though this statement was not extremely detrimental to the security of the shipment, it was information that needed to be controlled. Additionally, the information regarding this recovery was communicated to many people within the licensee's facility. The Radiological Safety Officer revealed that he had communicated the dates and other details of this shipment with the management of the facility for their awareness. It is understandable that an organization would want situational awareness, but this information could aid an outside adversary team. Also, the team that conducts these recoveries carried a list of future location shipments and dates with them. This information on one recovery was left unattended in a vehicle.

2.4 PHYSICAL SECURITY SYSTEMS

Physical security systems are the primary protection against plots that exclusively involve outsiders, but these same systems can be used to mitigate the insider. These systems should be designed to detect, delay, and respond to the unauthorized access of the materials or conveyance. A comprehensive system will combine engineered controls with administrative controls to detect insider and outsider adversary actions. By employing locks, trailers, and secure containers along with other barrier technologies, the time delay an insider would have to overcome to remove material would increase, increasing the probability that a response force would arrive in time to stop the adversary force.

The lack of robust physical security controls on a consistent basis among the different carriers results in inconsistent physical security practices within the industry. In addition, this lack of robust physical security controls on the conveyance allows the insider to compromise the system with ease. Despite the fact there are some physical or engineered security controls in place, there is a definite need for a more robust physical security system package for these shipments. Also, the response to an act of theft or sabotage against one of these shipments can take an extraordinarily long time because of the current protocols in place.

3. RECOMMENDATIONS

To address concerns regarding insider threat, a layered defense strategy consisting of policies, procedures, and engineered controls must be implemented. In addition, organizations need to pay close attention to their business policies and procedures, organization culture, and their operating environment (Cappelli, Moore, Shimeall, & Trzeciak, 2009). Organizations that operate within the radiological transportation industry appear to be compliant with requirements from a regulatory perspective, but these requirements are minimal and do not adequately address the threat. Regulatory compliance forces organizations to somewhat address risk and provides a basic level of protection, but best practices are something that organizations should strive for. However, essential practices should

be established before best practices can be achieved. A list of key essential practices to effectively address the insider threat is presented in this paper.

3.1 ESSENTIAL PRACTICE 1: A STRONG TRUSTWORTHINESS/PERSONNEL SECURITY PROGRAM

It is important that the industry reduce the threat by establishing a high level of assurance in the trustworthiness of personnel within the industry. The industry needs to see both the benefits and limitations of background checks and the advantages of using expanded background checks that can enhance its security program. This would include performing background checks with expanded data, conducting them on a more frequent basis, and integrating their trustworthiness program with an insider mitigation program.

Most of the OSRP personnel and drivers currently exceed the requirements that are set forth by both the Nuclear Regulatory Commission (NRC) and the TSA for background checks. Most of these individuals have at least an L clearance, but this is not always the case. There are instances where drivers may only have the HAZMAT endorsement, and others in the field only have a trustworthiness and reliability check. Furthermore, some individuals have only had an initial investigation when they were hired and have not had another background investigation since. Getting the industry to understand that this expanded data gathering for background checks is essential to build an effective security program.

To help achieve a more comprehensive trustworthiness/personnel security program, it would be beneficial for Office of Radiological Security (ORS) to require that employees and the contractor/subcontractor employees who have a role in the OSRP process have a security clearance. One way to implement this requirement is to include in the contracts that all employees or subcontractors will have a security clearance.

3.2 ESSENTIAL PRACTICE 2: INSIDER THREAT MITIGATION PROGRAM

To address the insider threat, organizations need a program that outlines the basic steps that can be undertaken to employ a risk management strategy and mitigation plan specifically aimed at the insider. The program must be supported by both a policy and training for the threat. While policy is a critical element for preventing and responding to insider threat, policy alone is not enough. Awareness and education about the threat of insiders, a policy that addresses insider threats, and a program in place to address the threat are also critical elements. To address the insider threat, the following steps could be put into place.

To assist in developing an insider threat program for the commercial industry, ORS could help lead this initiative. This initiative could be a coordinated effort designed to proactively help develop and educate organizations about what an effective insider threat program within the radiological transportation industry would look like and how to implement the program. This program could be established and enhanced by the inclusion of a stakeholder forum. This forum would bring together government, industry, public officials, and academia to devise a strategy to build an insider threat program, share information, and share information on best practices aimed at protecting the industry and the public from emerging insider threats. The program should highlight the need to do the following.

- Implement an internal policy to mitigate the insider threat
- Develop and implement a continuous monitoring program
- Develop and deliver training describing what an insider threat is, what indicators to look for, and how to respond and report a potential insider threat

- Institute a culture and training program emphasizing to employees that the organization has a right to monitor their activities in the workplace and on the organization's networks

In addition, to build upon this effort, private organizations should build an insider threat program within their own organizations. This program should strive to protect an organization's sensitive and critical information as well as the assets they transport. The program should include organization-wide participation and components such as standard operating procedures for assessing, reporting, and responding to insider threats and insider threat training and awareness (United States Postal Service Office of Inspector General, 2018). Additionally, organizations should do the following.

- Evaluate who has access to the critical assets/ processes and information
- Decide if additional monitoring or scrutiny is prudent for those positions where key access or knowledge is needed
- Implement a continuous monitoring process (periodic background checks of high-risk positions)
- Determine the best way to implement an insider threat program
- Conduct insider threat training internally

Table 1. Recommended ORS Insider Threat Program

Focus Areas	Recommendation for Insider Threat Program
Program Management	• Create and implement policies related to insider threats • Develop a tiered approach for background checks
Incident Response	• Establish an Insider Threat Program that includes specific procedures for responding to potential incidents involving insiders
Training	• Conduct Training that includes the following. o Specific information about insider threats and information on mitigating the insider threat o Teach employees on their requirement to report potential insider threats and how to report concerns o Encourage employees to use secure means for transmitting information and ensure good information security practices are followed
Information Security	• Develop a program where organizations ensure that personnel are properly transmitting and handling sensitive information
Technical Controls	• Develop a continuous monitoring program to detect and respond to at-risk insider behavior

3.3 ESSENTIAL PRACTICE 3: INFORMATION PROTECTION

The protection of information is crucial in any program where information needs to be tightly controlled. Information protection is one of the most effective ways to mitigate the insider. To address this area, an information security policy should be implemented in organizations that play a role in transporting these materials. An effective information security program cannot be established without increasing employee awareness and implementing a

training program to address policies, procedures, and tools. The protection of information is a requirement, but organizations need to continuously work to ensure that personnel are reminded that information related to shipments, security plans, and responses need to be controlled on a need-to-know basis. Additionally, it should be stressed that the information not only needs to be protected externally but also internally.

ORS could assist in this effort by raising awareness of the issue, providing training to the industry at the stakeholder's forum, and requiring entities that conduct work within the OSRP program to have an information security program.

3.4 ESSENTIAL PRACTICE 4: ROBUST PHYSICAL PROTECTION SYSTEMS

There is a need to enhance the security profile of conveyances by significantly reducing the conveyance vulnerabilities to insider actions which can seriously degrade system effectiveness. To address the insider threat, physical security systems should consist of a system that includes a comprehensive, multifaceted approach, rather than depending on stand-alone systems. Ultimately, the effort should be to maximize the scale and complexity of the systems so that both insiders and outsiders would have to use more sophisticated means to defeat the total system. To accomplish this, results from the assessment that ORNL is conducting regarding physical security upgrades for the trucks and trailers that transport radiological material should be implemented along with the other recommendations outlined in this paper. Although a strong insider mitigation program is critical, the protection strategy needs to be complemented with a robust physical security system. Elements for success can be accomplished by developing technical and nontechnical capabilities to (1) deter adversary actions; (2) detect unauthorized activities; (3) delay unauthorized activities; (4) mitigate unauthorized activities; and (5) respond to unauthorized activities.

It would be beneficial to consider the analysis results of the most common physical protection systems (PPS) deployed in the radiological transportation industry and determine what the best practices are and where effective upgrades can be made. This evaluation should include a review of operations and conditions as well as a review of the conveyances and containers used for transport.

Once this analysis is complete, recommendations for upgraded PPS packages which integrate people, procedures, and equipment for the protection of the assets should be developed. To effectively build a security system, we must look at much more than just getting the right technology. This upgraded system should be designed to protect against all the threats such as terrorist, criminal outsiders, disgruntled employees, and insiders (Garcia, 2008).

4. CONCLUSION

Insider threats and the attacks they can carry out can be fatal to both an individual business and the industry. It is vital that organizations understand that security is a function of business and that organizations have a business-first attitude regarding the security issues they face. Developing an effective trustworthiness program that includes an insider threat program along with the control of information and upgrading the physical security systems on vehicles that transport radiological materials present a new level of transportation security that does not currently exist. Adding these important aspects of security allows the industry to strengthen the radiological transportation security arena. As the adversary develops new, more sophisticated methods to attack, it will only become easier for insiders to perpetrate an attack on radiological shipments. Even though these upgrades are not a guaranteed way to eliminate the insider threat, making stakeholders aware of the threat and that it exists, as well as implementing both technological and nontechnical means to mitigate the threat, is increasingly important.

Finally, an effective security program to enhance the radiological transportation industry will require an understanding of risks and balancing the following three critical elements.

- **Stakeholder training and participation** in security enhancements
- **Organizational policies, procedures, and processes** that address specific needs and that are well written, complied with, routinely audited, and kept current
- **Security technologies** that are designed, purchased, and installed based on an assessment of need, properly utilized, monitored, and maintained

It is important to get the industry to understand that effective security is not conducted just once; radiological transportation security must be maintained and continually improved. Sustaining security in the radiological transportation sector requires both capacity and commitment. Most likely, assistance programs to help build capacity in this sector will be needed as well as assistance with commitment building. Convincing the private sector that it is in their best interest to take the actions needed to sustain effective security for the long haul will take dedicated effort (Bunn, 2013).

5. REFERENCES

Ananthanpillai, R. (2015, July 23). Insider Threats and the Limitations of Pre-Hire Background Checks. Retrieved from http://www.riskmanagementmonitor.com/insider-threats-and-the-limitations-of-pre-hire-background-checks/.

Brody, R. G., & Cox, V. L. (2015). Background Investigations a Comparative Analysis of Background Checks and Federal Security Clearance Investigations. *Business Studies Journal*, 84–94.

Bunn, M. (2013). Strengthening Global Approaches to Nuclear Security. *Proceedings of the International Conference on Nuclear Security: Enhancing Global Efforts, International Atomic Energy Agency (IAEA).* Harvard.

Bunn, M., & Sagan, S. D. (2014). *A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes.* Cambridge, Mass.: American Academy of Arts and Sciences.

Cappelli, D., Moore, A., Shimeall, T. J., & Trzeciak, R. (2009, January). *Common Sense Guide to Prevention and Detection of Insider Threats 3rd Edition – Version 3.1.* Retrieved from https://clearwatercompliance.com: https://clearwatercompliance.com/wp-content/uploads/CERT_common_sense_guide_to_prevention_and_detection_of_insider_threat s.pdf.

Garcia, M. L. (2008). *Design and Evaluation of Physical Protection Systems.* Boston: Butterworth-Heinemann.

Gitomer, S. J., O'Brien, H. A., Mason, C. F., Strub, T. L., & Van Tuyle, G. J. (2003). Reducing RDD Concerns Related to Large Radiological Source Applications. Los Alamos: Los Alamos National Laboratory.

Hill, E. (2012, November 12). *Kill the Password: A String of Characters Won't Protect You*. Retrieved from https://www.wired.com/2012/11/ff-mat-honan-password-hacker/.

Izurieta, S. (2018). Reducing the Impact of Unmanaged Insider Risk Through Continuous Evaluation. *Security Magazine*.

Jones, G. S. (2016, June 3). *ISIS and Dirty Bombs.* Retrieved from www.rand.org: https://www.rand.org/blog/2016/06/isis-and-dirty-bombs.html.

Los Alamos National Laboratory. (2018). *What is the OSRP?* Retrieved from https://osrp.lanl.gov/what_is_osr.shtml.

McBride, T. W. (2008, February 15). *Probable Economic Targets for Terrorism by Radiological Attack.* Retrieved from http://www.au.af.mil: http://www.au.af.mil/au/awc/awcgate/awc/2008_mcbride.pdf.

Rose, R. N. (2016, August 30). *The Future of Insider Threats.* Retrieved from Fobes.com: https:// threats/#6e66512e7dcb.

Sandia National Laboratories. (2015, November 3). *Insider Threat Awareness.* Retrieved from www.sandia.gov: https://www.sandia.gov/FSO/docs/SEC105.pdf.

Timmins, A. (2013, June 09). *N.H. Looks at Including Mental Health Records in Gun Background Checks*. Retrieved from https://www.vnews.com/Archives/2013/06/a1MentalHealthMonitor-epk-vn-060913.

U.S. Chamber of Commerce. (2010, October 21). *Homeland security and defense issues.* Retrieved from https://www.uschamber.com/cyber-intelligence-and-security-division.

U.S. NRC. (2014). *Physical Security Best Practices for the Protection of Risk-Significant Radioactive Material.* Washington, D.C.: U.S. NRC.

United States Government. (2012, July 01). *Part 147—Adjudicative Guidelines for Determining Eligibility for Access to Classified Information.* Retrieved from https:// part147.xml#seqnum147.8.

United States Postal Service Office of Inspector General. (2018, September 18). *Insider Threat Program Audit Report IT-AR- 17-007.* Retrieved from https://www.uspsoig.gov/document/insider-threat-program/.