Considering insider threat security risks for radioactive materials below quantities of concern.

A Pilot Examination of the Methods Used to Counteract Insider Threat Security Risks Associated with the Use of Radioactive Materials in the Research and Clinical Setting

B.G. Tsenov, R.J. Emery,* L.W. Whitehead,* J. Reingle Gonzalez,* and G.L. Gemeinhardt†*

Abstract: *While many organizations maintain multiple layers of security control methodologies to prevent outsiders from gaining unauthorized access, persons such as employees or contractors who have been granted legitimate access can represent an "insider threat" risk. Interestingly, some of the most notable radiological events involving the purposeful contamination or exposure of individuals appear to have been perpetrated by insiders. In the academic and medical settings, radiation safety professionals focus their security efforts on (1) ensuring controls are in place to prevent unauthorized access or removal of sources, and (2) increasing security controls for the unescorted accessing of large sources of radioactivity (known as "quantities of concern"). But these controls may not completely address the threat insiders represent when radioactive materials below these quantities are present. The goal of this research project was to characterize the methodologies currently employed to counteract the insider security threat for the misuse or purposeful divergence of radioactive materials used in the academic and medical settings. A web-based survey was used to assess how practicing radiation safety professionals in academic and medical settings anticipate, evaluate, and control insider threat security risks within their institutions. While all respondents indicated that radioactive sources are being used in amounts below quantities of concern, only 6 % consider insider threat security issues as part of the protocol review for the use of general radioactive materials. The results of this survey identify several opportunities for improvement for institutions to address security gaps. Health Phys. 114 (3):352–359; 2018*

Key words: *operational topics; contamination; radiation risk; risk analysis*

INTRODUCTION

The examples of intentional contamination of food and drink have occurred with ^{32}P and ^{125}I in research laboratories in prestigious academic institution such as National Institute of Health (NIH), Massachusetts Institute of Technology (MIT), and Brown University. These examples demonstrate that while a complex system of people, procedures, and equipment, called Physics Protection System (PPS) offers protection against an external threat, such systems may not be satisfactory to address threats from inside the organization (Federal Register 1996; U.S. NRC 2012, 1998; Waller and Maanen 2015). This series of events associated with security of radioactive materials has led to a change in the primary roles of health physicists (HP) from control and surveillance of these sources to now also addressing the insider threats which are much harder to detect and control. While source security was in the radiation protection regulations long before these events a new change of radioactive materials security perspective was triggered after September 11, 2001 (10 CFR 20.1801 and CFR 20.1802) (U.S. NRC 1991).

The threat that terrorists are planning to use radioactive materials became apparent especially after the arrest of an American citizen, Jose Padilla on suspicion of plotting a radiological bomb ("dirty bomb") attack (Zimmerman and Loeb, 2004). According to U.S. intelligence during 2001 and early 2002, Padilla was trained in the

**The University of Texas School of Public Health, Department of Epidemiology, Human Genetics and Environmental Sciences, 1200 Pressler Street, Houston, TX 77030; †The University of Texas School of Public Health, Department of Management, Policy and Community Health, 1200 Pressler Street, Houston, TX 77030.*

The authors declare no conflicts of interest.

Boris Tsenov has over 15 years of experience in radiation safety. At his last position as a radiation safety specialist at the Environmental Health & Safety department of the University of Texas Health Science Center at Houston he supported the broad scope permit for the research and medical use of radioactive materials, medical and research use of x rays and lasers. He earned his doctorate of public health in occupational health from The University of Texas at Houston School of Public Health. He earned his M.S. in nuclear engineering from Sofia University. Currently, he lives in Germany and specializes in medical photonics. His email is **bgtsenov@gmail.com**.

construction and deployment of a weapon, which would use conventional explosives for the dispersion of radioactive materials a device called a "radiological dispersal device" or a "dirty bomb." In academic and medical institutions, radioactive materials in quantities of concern may be present as the radioactive sources in self-shielded irradiators, which usually have a ^{137}Cs radioactive source with activity higher than 9.99×10^{13} Bq. Thus, in 2006, the U.S. NRC issued Increased Control (IC) orders (EA-05-090) to certain licensees for implementing interim security measures (beyond those previously required) to prevent unauthorized removal or access of these materials. Under the IC orders, licensees were required to increase security over such radioactive sources in order to prevent unintended radiation exposure or malicious acts (U.S. NRC 2007). An example is the Trustworthy and Reliable (T&R) determination, which includes fingerprinting and review of criminal history, personal references, work history and education for approval of unescorted access to radioactive materials under the IC licensees. However, the IC order does not apply to most of the radioactive materials used in research and in clinics, since typically the amounts used are below the established quantities of concern. Issues regarding those materials in amounts below the quantities of concern are the focus of this study, as security measures for these may not be sufficient or considered in an organized manner.

RESEARCH OBJECTIVES AND AIMS

This study sought to identify whether radiation safety professionals have completed any formal training regarding security through a web-based survey. Furthermore, this study sought to:

1. Identify the most commonly used methods to counteract insider threat security risks associated with the use of radioactive materials in research and clinical settings;
2. Identify gaps within these commonly used control methodologies; and
3. Propose recommendations for needed security elements, which could be included in an institutional insider threat risk mitigation plan and related training.

METHODS

The survey for this project contained 28 questions. These questions were developed based on commonly used controls for counteracting misuse of radioactive materials in the Texas Medical Center (TMC) and other academic and medical institutions at which the first author held appointments. Such controls usually are established in accordance with the institution's Protection of Assets Manuals.

Prior to distribution of the survey, the survey was piloted to ensure that the questions were well formulated and understood by respondents and whether the size/content of the survey required adjustment. Members of the News in RadiatioN (NiRDs) group were recruited to participate in the pilot to obtain initial feedback. NiRDs is an informal group of radiation safety professionals from the TMC, Houston, Texas, who meet quarterly. TMC is the largest medical center in the world and consists of sixty-nine academic, medical and health care providing institutions, many of which use radiation producing devices and radioactive materials. The pilot aimed to identify misleading questions or poor instructions for further editing or removal from the survey tool.

STUDY DESIGN AND SETTINGS

The study design is a descriptive cross-sectional study of radiation safety professionals in academic and medical settings. The study was conducted during the summer of 2016 involving an electronic web-based survey distributed to radiation safety professionals via the Academic and Medical Radiation Safety Officer (AMRSO) listserv. At the time of the survey the listserv had approximately 700 professionals, employed full or part time at academic and medical institutions. According to the listserv moderators, AMRSO listserv has a limit of two members per institution, which corresponds to 350 institutions represented. This group "is not affiliated with the Health Physics Society (HPS) nor the RSO Section of the HPS" (AMRSO 2016). However, many of the members of the listserv are Certified Health Physicists (CHPs) and/or members of the HPS, and thus support was sought and obtained from the South Texas Chapter of the Health Physics Society (STC-HPS) to emphasize the importance of this topic to the radiation safety profession. The web-based survey tool (SurveyMonkey) was disseminated to collect the data. All responses were anonymous and no IP addresses were collected. To address the human subjects' issues, the pilot and survey were approved by University of Texas Health Science Center at Houston Committee for the Protection of Human Subjects (CPHS).

DATA COLLECTION

The survey was distributed electronically to the participants via the AMRSO listserv, and participation was voluntary and without tangible incentives. Participants were provided with a detailed explanation of the study, its objectives and informed consent, in a cover letter. The letter requested only one radiation safety representative from an institution to be designated as a respondent. The survey took no longer than 20 minutes to complete.

DATA ANALYSIS

Simple descriptive statistics were used to analyze the survey results. Chi-square analyses with Fisher's Exact tests were performed using Stata

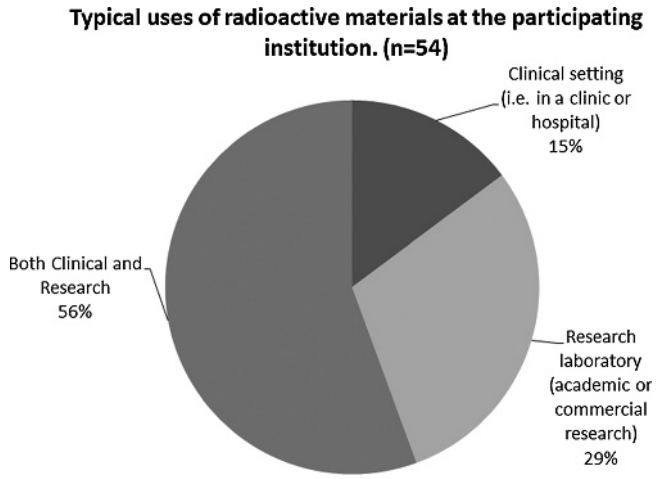

FIG. 1. Percent of institutions by typical use of radioactive materials.

14 (College Station, Texas) to compare the response percentages. The results also were graphically presented using Microsoft Excel charts.

RESULTS

The survey was available online for four weeks between August 5th and September 2nd in 2016 and a total of 78 survey responses were received. Of these responses, 22 were omitted (one participant declined to provide informed consent and 21 attempted, but did not complete the survey), resulting in 54 analyzable surveys. Two reminders were sent by the author during the survey period and one or two days before the closing date of September 2, 2016. Forty-two (78%) participants identified themselves as Radiation Safety Officers, 4 (7%) as Radiation Safety Managers, 3 (6%) as Assistant Radiation Safety Officers, and 1 as a Radiation Safety Specialist. Under the answer "Other," three participants described their positions as Assistant VP for University Health and Safety, EH&S Associate Director and a Physicist/RSO.

All respondents were individuals from institutions in the United States. Forty-eight (89%) were from large institutions with more than 1,000 full-time employees and 20 (38%) of the Radiation Safety groups represented consisted of more than five full-time employees. At eight (15%) of participants' organizations there were no attending students. Almost all [52 out of 54 (96%)] of the respondents indicated that their organizations possessed radioactive materials used for clinical applications or biomedical research, and only two responded that their organizations possessed SNM or IC materials. As shown in Fig. 1, more than half of the respondents (n = 30) indicated that these materials were typically used in both clinical and research settings, followed by research laboratory use in 16 cases. Eight participants used the materials only in a clinical setting (Fig. 1).

Forty-seven of the survey respondents (87%) indicated that their radiation safety committee does not consider insider threat issues within the context of their charge for protocol reviews (Fig. 2). Further, when the security risk assessment was performed for insider threat, 23 (42%) of the respondents indicated that they do not have a reviewer on the committee knowledgeable in criminal activities, behavioral assessment, and/or security training. Twenty-one (39%) of the respondents considered such reviewer's expertise was "not applicable" (Fig. 3), and only 7 (13%) had at least one reviewer with these qualifications.

When asked to consider an ideal security program that includes insider threat consideration, the respondents selected security personnel knowledgeable in electronic and physical access as the most important expertise, followed by a policeman or expert in background checks. These were followed by individuals knowledgeable in suspicious behavior identification, an insider threat safety trainer, occupational health physicians (knowledgeable in first aid, exposure/internal contamination assessment, etc.), and, finally, an expert (psychologist/psychiatrist or other) in charge of the Behavioral Intervention Team (Fig. 4). Participants reported that most institutions do not have a mechanism in place to assess whether the concentration of radioactive materials has decreased when

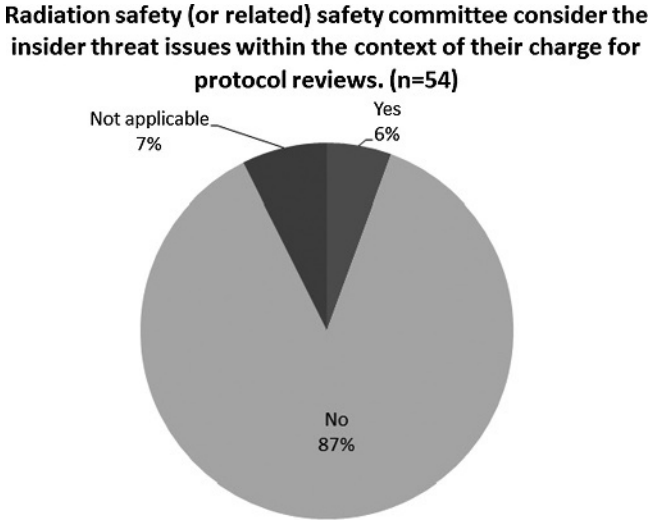

FIG. 2. Percent of respondents reporting that insider threats are considered during protocol review.

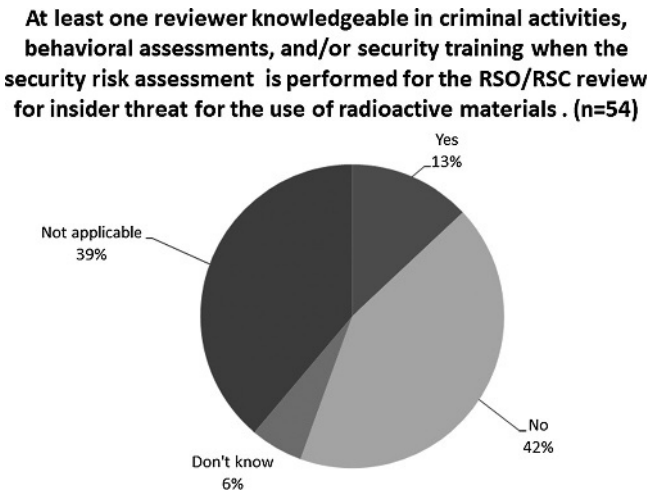

FIG. 3. Percent respondents reporting that at least one reviewer is knowledgeable in criminal activities, behavioral assessment and/or security training.

the volume within the vials remains constant. This answer was provided by 43 (80%) of the participants (Fig. 5). Twenty-one (39%) of the respondents indicated that the RSO will receive a notice from the radiation workers when an experiment involving radioactive materials produced unexpected results that suggest either an absence or decreased amount of the material (Fig. 6). However, most of the participants (n = 43 or 80%) responded that the radiation safety staff specifically inquire about any safety or security concerns as part of the radiation safety inspections.

Just over half of the radiation safety professionals (n = 29 or 54%) indicated that they have been trained on specific insider threat oversight, security risk assessment, or other security considerations. Participants from six institutions (11%) responded that their radiation safety training specifically addresses the necessary security controls of radioactive materials. The "insider threat" risk factor and threat mitigation, however, is not included in the basic radiation safety training according to almost all (52 out of 54) the participants (Fig. 7). Finally, 28 (53%) of the respondents consider additional training on insider threat security issues as helpful to them and their radiation safety program, 8 (15%) disagree, and 17 (32%) are not sure about the benefit of such training.

Based on collected data, the survey results were organized in subgroups and evaluated further. Chi-square analyses with Fisher's Exact tests were performed using Stata to compare the response percentages. These subgroups were based on types of institution (i.e., whether radioactive materials were used in academic research, clinical application, or both). The author compared organizations with established background check practices (for the users of radioactive materials below the quantities of concern) to those without established background check practices and based on whether there were students attending the participating institution or not. Specific response percentages were compared between the type of institutions and those who perform background checks for their radiation users. Response percentages were also compared between the educational institutions (with students attending/present) and again if background checks were performed or not. Additional analyses were done for those RSOs who have received training in insider threat security and type of institution as well as those institutions where insider threat is considered by radiation safety committee. There was no significant difference in use of radioactive materials based on background check practices in the institutions, χ^2 (df = 4, n = 54) = 3.33, p = 0.5034 (Table 1). However, significantly different effects were observed between institutions with established background check practices and those without established background checks when compared with those where there are students attending, χ^2 (df = 2, n = 54) = 6.4468, p = 0.04 (Table 2). The absence of students was related to a much higher relative occurrence of background

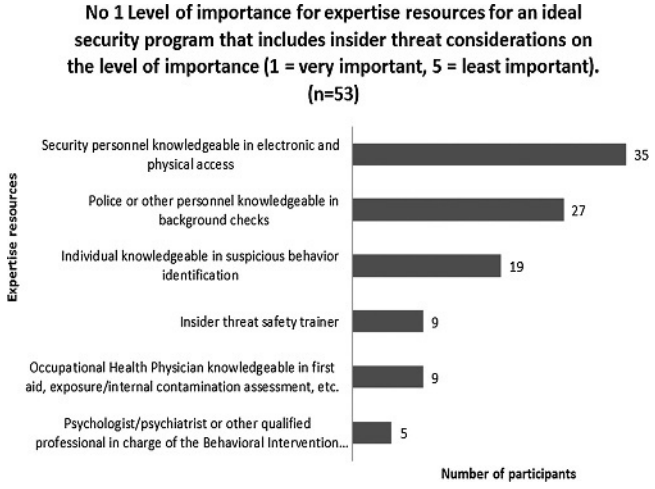

FIG. 4. Number of respondents reporting priority of various expertise for ideal insider threat security programs.

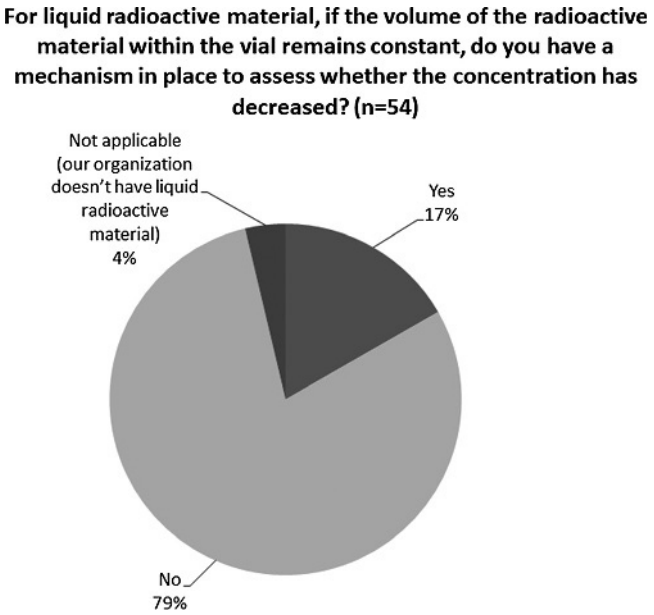

FIG. 5. Percent of respondents reporting a volume vs. concentration verification method for liquid radioactive materials.

checks, compared to settings where students were present.

DISCUSSION

Radiation safety professionals today play a very active role about safeguards of radioactive materials in quantities of concern due to the recently adopted Increased Control (IC) regulations. In most academic and medical institutions, multiple controls are in place for securing the radioactive materials from external or internal threats (Table 3).

The results of this survey, however, show that for general radioactive materials (below the quantities of concern in Categories 1 and 2) gaps exist in three major parts of the participating institutions' security programs. These are the risk assessment process, the training of the radiation safety officers, and the use of resources needed to counteract insider threat security risks. For example, almost half (46%) of the participating RSOs had never been trained on insider threat oversight, security risk assessment, or other insider threat security considerations.

Often, radiation safety professionals deal with a mixture of security controls at different sites where both types of materials are used (i.e., general unsealed sources and sources of concern) and thus in many cases the increased control measures are not applied in every research laboratory or storage spaces. Therefore, the need exists for such gray areas to be identified and a novel approach to be adopted in the institutional oversight committee for the sources below the quantities of concern, where the gap is found.

The survey results revealed that key resources are either missing or not clearly understood by the radiation safety professionals. One example was not knowing to whom suspicious behavior should be communicated within the organization. For most of the participants, reports should be made to the institutional compliance officer; however, only a few participants were familiar with the institutional behavior intervention team. These resources seem similar but the compliance office was usually approached when a policy or procedure was violated. The institutional behavioral intervention team, on the other hand, tracks the "red flags" over time, detecting patterns, trends, and disturbances in individual or group behavior (NBITA 2017). It is important to recognize the difference between these two oversight mechanisms because the security considerations for the personnel are focused on the behavior, not assumptions or presumptions (Engells 2013).

It was surprising that the dual use of the radioactive materials below category 1 and 2 (their potential to cause harm) rarely were considered as a security concern during the risk assessment process. This comes as a surprising finding because such materials were used in several malicious acts, including food and drink poisoning (Federal Register 1996; U.S. NRC 2012,

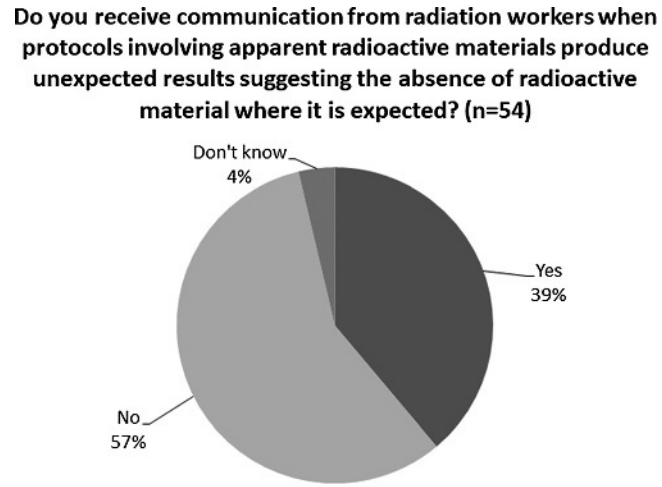

FIG. 6. Percent of respondents reporting communication of unexpected results suggesting the absence of radioactive materials.

FIG. 7. Percent of respondents reporting insider threat as part of the basic radiation safety training.

1998). Even though radioactive materials in quantities used for scientific research or in clinics would probably not cause immediate death or severe injury if misused, misuse could damage the public trust and the institution's reputation. Possibly, this gap of knowledge explains why, at most (52 out of 54) of the institutions, the insider threat issues were not considered during the radiation safety committee protocol review for the general radioactive sources.

For many of the RSOs, the ideal insider threat security program needs three important resources (Table 3). First, RSOs would like to have available on the radiation safety committee the expertise of police or an individual knowledgeable in electronic and physical access. From the additional responses received, it was evident that when both types of radioactive materials are present (in quantities of concern and below), there are some areas where the access was organized with electronic keys and in other areas there are different controls in place, such as key pads or metal keys. Therefore, many respondents could not give a "yes" or "no" answer when asked if the access attempts after hours are tracked by the radiation safety professional, since a mixture of controls were used. However, the survey questions specifically asked for the security controls in areas where radioactive materials below category 1 and 2 were present and this was clarified and accented with the survey reminders sent to the listserv. This finding suggests that most of the RSOs feel the need for further expert evaluation of insider threats on the access controls for general radioactive materials. The second and third most desired resources for an ideal insider threat security program were experts in background checks and someone knowledgeable in identifying suspicious behavior. Results from the survey suggested that individuals with such expertise were available and present during the protocol evaluation process at only seven institutions. This was not surprising and supports the notion that most institutions do not perform reviews for insider threat when the radioactive materials were below the quantities of concern.

The overall survey response rate (15%) was reasonable, when compared to other similar web-based studies where the final response rate varied from 12% (Patlovich et al. 2015) to 30% (Harvey 2014). However, this response rate was lower than the projected and there are several issues that might have impacted the results. The first is the hesitancy of respondents to share security-related information. Security of radioactive sources is an area that most radiation safety professionals are advised to not discuss publicly out of concern that some specific information may lead to a breach of security. To assure trustworthiness, support was provided by one of the founders of the AMRSO listserv and the survey link was sent out by another respected member of the listserv. The second important issue for the lower response rate was believed to be the problems respondents had initially with the survey link. After multiple complaints in the first week when the survey was launched, the survey platform SurveyMonkey investigated and responded that the link

Table 1. Percentages for type of institution by background checks, (n).

	Background checks		
Type of use	Yes	No	Total
Research and clinical	24 (13)	30 (16)	54 (29)
Research	8 (4)	20 (10)	28 (14)
Clinical	7 (4)	6 (3)	13 (7)
Total	42 (21)	58 (29)	100 (50)

Chi Square 1.79.[a]
[a]$p = 0.435$ — Fishers exact test is reported because chi square isn't stable with cell sizes smaller than 5.
Note: Number in parenthesis are frequency of answers in each category.

Table 2. Percentages for students attending status, by background check status.

	Background checks		
Students attending	Yes	No	Total
Students	28 (15)	52 (28)	80 (43)
No students	12 (6)	2 (1)	14 (7)
Total	42 (21)	58 (29)	100 (50)

Chi Square 6.3851.[b]
[b]$p = 0.03$ — Fishers exact test is reported because chi square isn't stable with cell sizes smaller than 5.
Note: Number in parenthesis are frequency of answers in each category.

Table 3. Elements most needed and prevailing control mechanism in the security programs of the participating institutions.[a]

During the insider threat risks assessment process, the most needed element is access to Police/Security personnel with knowledge in:
• Electronic and physical access
• Background checks
• Suspicious behavior identification.
Prevailing practices regarding the criminal background checks:
• Criminal background checks are part of the hiring process for all employees
• Background checks extend beyond criminal history to aspects such as credit history, driver history or confirmation of academic credentials
The most common oversight mechanisms currently in place with regard to the security of radioactive materials:
• Collaboration with the local law enforcement agency to respond to potential threats
• Mechanisms in place for people to report suspicious behavior to an Institutional Compliance Officer (or equivalent)
• Assessments are performed regarding the security of the radioactive materials
• Radiation Safety Surveys include a section on security measures
• Formal mechanisms exist for persons to be able to report security concerns or suspicious behavior to the Radiation Safety Officer

[a]This is not all-inclusive list, but rather a list of the most preferred expertise and often utilized controls.

was functional. Representatives from SurveyMonkey suggested the respondent clear cache and cookies on their browsing settings and try again. Many of the respondents could copy and paste the link into another browser and complete the survey. Regardless of the troubleshooting and the received support, participants who opened the link and agreed to the informed consent may have been discouraged (n = 21) from completing the survey in full by the topic sensitivity.

The listserv allows only two members from each organization. However, it is possible that more than two individuals from an organization could be existing members such as safety specialists, or other staff members involved in insider threat risk prevention. Therefore, selection bias, which is a common issue with web-based surveys, may have impacted the sample's representativeness of the target population (Aday and Cornelius 2006). Another factor potentially driving the lower response rate could be that the survey was sent in August (2016) when some members were on their summer vacation. In addition, some attrition may have occurred simply because the survey was too long (28 questions).

CONCLUSION

Radioactive materials below Category 1 and 2 are used in many research laboratories (academic or commercial), clinics and hospitals around the nation by employees, students and contractors. Coincidently, in the same month when the reported survey was performed, a GAO report (U.S. GAO 2016) stated security vulnerabilities remain for radioactive material sources in Category 3 and below. This observation from the GAO report aligns with the importance of this research project. According to the survey results, 87% of radiation safety professionals during their protocol review did not consider that a radiation worker with legitimate access to these materials could become a malicious insider. This represents a risk for the institution's assets, reputation, and the employees' health, especially since all the reported cases of the misuse of general radioactive materials occurred in academic, research, and medical settings. The survey results indicated that there are well established security practices due to the increased control regulations for the sources in quantities of concern. However, it was evident that wherever combinations of control methodologies were present (for general sources and for quantities of concern), there was no uniform approach for the background checks and for monitoring the radiation workers' actions or behaviors when no one was present.

In conclusion, there is a need to develop formal training for radiation safety professionals on the topic of insider threat security risks for the sources in Category 3 and below. This training should include details such as causative factors, preventive measures, and a comparison of the prevailing methods used to counteract insider threat security risks in academic and medical settings with the methods used in other settings with highly valuable commodities.

Acknowledgments—The authors wish to express their sincere appreciation for the support provided for this research by the leadership and staff of the University of Texas Health Science Center at Houston Radiation Safety Program, and all of the radiation safety professionals who participated in the survey.

REFERENCES

Academic and Medical Radiation Officer Group. The RSO Section of the Health Physics Society. Available at ***www.hps1.org/sections/rso/ophpinfo/AMRSO.htm***. Accessed 4 October 2017.

Aday LA, Cornelius LJ. Design and conducting health surveys a comprehensive guide. San Francisco: Jossey-Bass; 2006.

National Behavioral Intervention Team Association. Behavioral intervention teams. 2017. Available at ***https://nabita.org/behavioral-intervention-teams***. Accessed 4 October 2017.

Engells TE. The insider threat—A new aspect of biosecurity. J Health Protect Manage 29:16–25; 2013.

Federal Register. Report to congress on abnormal occurrences which occurred between July and September 1995, 3rd Event: NIH Incident. Federal Register 61: 7123–7124; 1996. Available at ***www.gpo.gov/fdsys/pkg/FR-1996-02-26/pdf/FR-1996-02-26.pdf***. Accessed 4 October 2017.

Harvey R. An approach to radiation safety department benchmarking in academic and medical facilities. ORS 108:S29–S36; 2014. DOI: 10.1097/HP.0000000000000212.

Patlovich SJ, Emery RJ, Whitehead LW, Brown EL, Flores R. Assessing the biological safety profession's evaluation and control of risks associated with the field collection

of potentially infectious specimens. Applied Biosafety 20: 27–40; 2015.
U.S. Government Accountability Office. Report to the Ranking Member, Committee on Homeland Security, House of Representatives. Nuclear Security. NRC has enhanced the controls of dangerous radioactive materials, but vulnerabilities remain. Washington, DC: U.S. GAO; GAO-16-330; 2016.
U.S. Nuclear Regulatory Commission. Standards for protection against radiation. Washington, DC: U.S. Government Printing Office; 10 CFR Part 20; 1991.
U.S. Nuclear Regulatory Commission. Preliminary Notification of Event or unusual Occurrence PNO-1-98-052, Intentional Ingestion of Iodine-125 Tainted Food (Brown University). 1998. Available at ***www.nrc.gov/reading-rm/doc-collections/commission/secys/1998/secy1998-276/1998-276scy.pdf***. Accessed 4 October 2017.
U.S. Nuclear Regulatory Commission. Security Orders and Requirements/NRC order imposing increased controls (EA-05-090). 2007. Available at ***www.nrc.gov/security/byproduct/ea-07-305-fingerprinting-order-for-ic-licensees.pdf***. Accessed 4 October 2017.
U.S. Nuclear Regulatory Commission. Ingestion of phosphorous-32 at MIT. 2012. Available at ***www.nrc.gov/reading-rm/doc-collections/nuregs/brochures/br0117/961.html***. Accessed 4 October 2017.
Waller EJ, Maanen J. The role of the health physicist in nuclear security. Health Phys 108: 468–476; 2015.
Zimmerman PD, Loeb C. Dirty bombs: The threat revisited. Defense Horizons 38:1–12; 2004.