

Counterintelligence Quarterly

July 2003



DOE's Radiological Assistance Program Supports Dept. of Homeland Security

By Donald J. Fingleton, Ph.D.,
Contributing Writer

(Seattle, WA —) As black smoke from an explosion still rises from an industrial area just south of Seattle's downtown, state and local authorities realize that terrorists have struck, contaminating the area with a radiological dispersal device (RDD), commonly referred to as a "dirty bomb." Soon after local officials detected radiation, an immediate call to state officials was made, who in turn notified the U.S. Department of Energy (DOE), National Nuclear Security Administration and its Radiological Assistance Program (RAP). Team members from DOE Region 8 RAP, and the Richland Operations Office are scrambled, leaving their jobs as health physics professionals for an unknown situation in Seattle. Within hours, the RAP team arrives on scene to help local, state and other federal authorities assess the situation.



Region 8 RAP entry to obtain air sample at exercise perimeter.

This was the scene as it played out when the U.S. Department of Homeland Security (DHS) recently conducted the largest homeland security exercise in U.S. history. Dubbed "TOPOFF 2" — the fictional events unfolded over five days beginning May 12 and involved more than 100 federal, state, local, private sector, and Canadian agencies and organizations. This full-scale exercise tested their ability to respond to an orchestrated, multi-point attack: the RDD explosion in Seattle and a covert biological attack in Chicago.

"TOPOFF 2 was well worth it," said Kathy Beecher, the RAP Region 8 Regional Response Coordinator. Her RAP teams were deployed 24/7 for the exercise duration, monitoring the extent of the radiological contamination using sensitive instrumentation, reviewing computer models predicting how the explosion

and winds distributed the radiological material, and working jointly with local, state and other federal agencies on making recommendations on further steps to be taken to minimize the hazards. She and her team have been deeply involved in the planning and preparation effort for the exercise for the past year. RAP assets from the Livermore Site Office and the Idaho Operations Office assisted by providing Team Leaders who were prepared to request their full teams. Integration of the three Regions in the field worked "great," according to Beecher. "This seamless integration is a testament to the close working relationships and camaraderie of the RAP teams throughout the DOE complex."

"We have to be prepared to respond

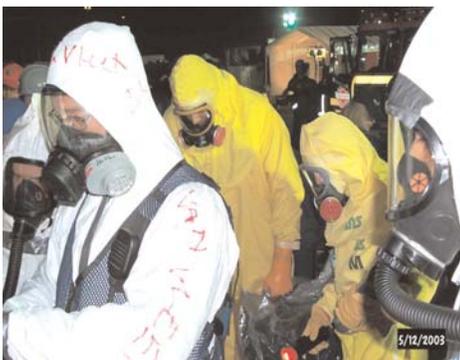
INSIDE THIS ISSUE

- 1 Radiological Assistance Program
- 2 Lab Employee Reports of Suspicious Incidents Continue to Protect Valuable Resources and Information
- 3 Foreign Intelligence Services: Coming to a Business Conference Near You

cont'd. on pg. 2

DOE's Radiological Assistance Program

cont'd. from pg. 1



Region 8 RAP making their initial entry with local responders.

to any real-life scenario that might occur," said DHS Secretary Tom Ridge. "TOPOFF 2 will provide us with concrete examples of how we can better respond to attacks."

DOE created the RAP in the 1950s to make DOE resources and expertise available to organizations responding to incidents involving radioactive materials. Deployed with their own equipment, the RAP team provides resources to evaluate, assess, advise and assist in mitigation of actual or perceived radiation hazards. During a terrorist event, these DOE assets are assigned to the DHS. The versatile DOE RAP teams were also deployed in the recent past in response to the major Cerro Grande fire near Los Alamos National Laboratory in 2000, and in support of the Federal Bureau of Investigation at the 2002 Winter Olympics in Salt Lake City, Utah.

Counterintelligence Training Academy Conducts New Counterterrorism/Counterintelligence Training for DOE Radiological Assistance Program Teams

While critically important for homeland defense, the well publicized TOPOFF 2 exercise could, according to some experts, inadvertently provide terrorists with an opportunity to gain a better

understanding of how state, local and federal authorities might respond to such a crisis, and how to counter those response activities in a real-life situation.

To protect against this, Christine Van Horn, RAP Regional Response Coordinator and Donald Krok, Senior Counterintelligence Officer from the DOE Chicago Operations Office are reviewing a more formalized approach for counterintelligence (CI) support for the RAP teams. "It is clear that CI and counterterrorism (CT) awareness training are needed to support the RAP mission," said Krok.

In response, Krok and Van Horn approached Tod Brown, Director, Plans, Policy, Training and Awareness Program in DOE's Office of Counterintelligence, seeking support for the development of a specialized CI/CT training program for this group. Brown tasked the DOE's Counterintelligence Training Academy (CITA) to develop a course of instruction which began as a collaboration between Van Horn, Krok, and CITA.

The result is an extensive course that covers CI/CT issues and addresses the handling and protection of classified materials, self protection techniques while on deployment, and/or operations at a crime scene, and how the DOE CI program can help reduce the risk of exploitation by foreign entities and crime elements. "Everyone involved must be aware of their surroundings, possible surveillance, and attempts to obtain information about our jobs or mission," said Krok. "This training provides the tools necessary to meet this responsibility."

The pilot course was presented to the Region 5 RAP team members (Chicago Operations Office) at Argonne National Laboratory-East last February, bringing the training to individuals directly, conserving RAP resources and funding. The pilot course is being formalized with the assistance of the Instructional Design

Team at the DOE Nonproliferation and National Security Institute and is ready for delivery to RAP teams across the country.

"The response has been great," said Van Horn. "Students rated the course as 'very good to excellent.'" Students have also commented on the training being helpful in terms of gaining skills to enhance their own personal security — on the job, on travel and at home.

For further information on the RAP training or other counterintelligence awareness training, contact your local counterintelligence office or the Counterintelligence Training Academy at 505/845-5170.

Lab Employee Reports of Suspicious Incidents Continue to Protect Valuable Resources and Information

By Jenna McCarthy

Posing as a representative of a local government in Latin America, an individual e-mailed a laboratory webmaster requesting information on a variety of narcotics, explosives, and counterterrorism-related technical products. The e-mail recipient, concerned about the unsolicited request, reported the incident to the local counterintelligence (CI) office. Further research by a CI officer revealed the individual to be a well-known drug trafficker connected to major narcotics cartels.

A family member of a laboratory employee was approached by an individual offering money in exchange for information concerning the laboratory. The incident was reported to the local CI office where further research revealed that the individual had ties to Iraq.

A plant security guard noticed a car pulled off to the side of the road taking pictures in the direction of a DOE facility. This incident was also reported to the local CI office but further

cont'd. on pg. 3

Lab Employee Reports of Suspicious Incidents

cont'd. from pg. 2

investigation revealed that, in this case, the individual had a hobby of photographing clouds; the facility was not the focus.

Seemingly suspicious incidents such as these, which may or may not be CI-related, happen more often than not. The continuous reporting efforts of DOE/NNSA employees prevent foreign intelligence services from gaining access to valuable resources and information through awareness.

In order to ensure that DOE/NNSA employees, information and resources are protected from foreign intelligence gathering efforts, the CI Program requires all employees, regardless of federal or contractor status, to report CI-relevant information. These requirements are intended to help counter the on-going efforts of foreign intelligence services, particularly those of sensitive countries, to collect sensitive and classified information. These intelligence services often foster professional and personal relationships as a means to obtain desired information. Accordingly, the requirements are in place to identify and clarify professional, personal and financial relationships DOE/NNSA employees might have with citizens of sensitive countries.

■ Who is considered a sensitive country foreign national?

A sensitive country foreign national is a citizen of, or employed by a government or institution of a sensitive country.

■ Why are countries designated as sensitive?

Countries are designated sensitive for reasons of national security, nonproliferation, anti-terrorism, and/or economic security. Due to the dynamic nature of world events, the sensitive country list may change periodically.

■ What types of contacts are employees required to report?

Employees are required to report:

Professional Relationships:

Professional contacts and relationships with sensitive country foreign nationals, whether the contact occurs at one's worksite or abroad.

Personal Relationships: Substantive personal relationships with sensitive country foreign nationals, other than family members. A substantive relationship is one that is enduring and involves substantial sharing of personal information and/or the formation of emotional bonds. Due to the subjective nature of "personal information" and "emotional bonds", each individual must judge as to the existence of, and a reporting threshold for, these criteria.

Financial Relationships:

Substantive financial transactions must be reported, whether they involve one-time interactions or on-going financial relationships. Partnerships or other business interests or investments are the focus of this reporting requirement since they provide the potential for exploitation or pressure.

Unusual Solicitations: Any attempts by unauthorized persons to gain access to classified information must be reported. Any attempts to obtain information, which can be in the form of pointed questions, subtle elicitation, or situations in which the DOE employee feels they are being targeted for exploitation. It applies to foreign nationals from sensitive and non-sensitive countries, as well as any other unauthorized persons, including U.S. citizens.

Anomalies: A foreign power activity or knowledge, inconsistent with the expected norm that suggests foreign knowledge of U.S. national security information, processes or capabilities.

■ Who do I contact?

DOE/NNSA employees should

report all incidents to their local CI office. Contact information is located on page four of this bulletin.

Foreign Intelligence Services: Coming to a Business Conference Near You

How Counterintelligence Awareness Can Protect You on Your Next Trip Abroad

By Dennis Fulkerson

My first business trip for the Department of Energy was to a scientific conference hosted in a non-sensitive foreign country. Prior to departure, I met with a Counterintelligence officer to receive a defensive counterintelligence foreign travel briefing. Having been on the project a very short time and recently out of school, I figured the threat the Officer described was non-applicable. This was, after all, an international conference hosted by allies of the United States.

Aside from the opportunity for foreign travel, I assumed this trip would be uneventful. However, a series of events unfolded. A fellow scientist from a non-sensitive country quickly became my friend and took me out for drinks when I arrived. During the conference, I noticed a group of wires leading from the conference room to an adjoining room. Upon asking, I was told they were taping the conference for those who were unable to attend; however, this was not disclosed at the start of the conference. At the end of the first day, anxious to go to my hotel room, I forgot my laptop in the conference room. Only to find the foreign security personnel found it and "secured it over night for me." On another occasion, when departing my hotel room for dinner, I left several papers spread out on my desk. When I returned to the room, they were neatly organized.

On the second day, another foreign colleague, who had similar interests in scuba diving, asked me to lunch. This colleague appeared to be a very popular and well known guest, as he was socializing with a number of other

cont'd. on pg. 4

Foreign Intelligence Services: Coming to a Business Conference Near You

cont'd. from pg. 3

individuals at the conference. I felt honored that he singled me out. By the end of the conference, the colleague invited me back to his country to do some diving and attend another conference, the subject of which happened to correspond with a project I was currently working on. During the week he introduced me to a delegate from a sensitive country who was also about my age. Coincidentally, the delegate seemed to have similar interests, hobbies (diving), education and current work assignments. The delegate appeared to be an open individual and discussed his own theories in detail. He continuously asked my opinion about projects he was working on but at no time made me uncomfortable or asked about any classified information. I was able to share my thoughts and opinions on his projects while making sure not to discuss what I was working on. After the conference, we spent a significant amount of time discussing diving and future goals; we shared business cards and contact information.

I returned from the trip and, per the CI officer's request, contacted him to let him know that there were no counterintelligence concerns. I made sure to mention that I was never asked about my project at a sensitive or classified level. Since that time I have received numerous e-mails from one of the individuals I met. We are planning a diving trip together in the next few months. However, although there were no inquiries regarding sensitive or classified information, past experience and mandated CI reporting requirements led me to continue to report the relationship and nature of the trips.

— Compilation of DOE/NNSA CI debriefing material gained from extensive interviews with DOE/NNSA professionals in routine Office of Counterintelligence return traveler debriefs.

This story may appear a bit far-fetched and unbelievable, but it is not. Situations such as this occur frequently during conferences both

here in the United States and during foreign travel. Social engineering and elicitation are the backbone for foreign intelligence services. In the espionage trade, elicitation is the term applied to subtle extraction of information during an apparently normal and innocent conversation. Conducted by a skillful intelligence collector, elicitation appears to be normal social or professional conversation and can occur anywhere: in a restaurant, at a conference or during an innocuous social event. Recording devices and surreptitious searches of items such as laptops and hotel rooms are also subtle ways of extracting information. Laptops left unattended can serve as a gold mine of information for foreign intelligence services. Elicitation and surreptitious searches require patience. Pieces of information are collected and put together over a period of time.

Oleg Kalugin, an ex-Soviet KGB agent, tells us that the Soviets used these techniques continuously to gain information from the United States and our personnel. A conference attended by foreign nationals provides the opportunity for these activities to take place.

So how can you protect yourself? The following are a few points to assist you when attending international conferences hosted by foreign nationals of sensitive and non-sensitive countries:

- You are not obligated to give information to unauthorized individuals, including personal information about you or your colleagues.
- Feel free to ignore any question you think is improper and change the topic.
- Deflect the question with one of your own.
- Give a nondescript answer.
- Suggest that you have to clear such discussions with your security office.
- Never leave your laptop or other electronic devices unattended.

- Lock all luggage and take valuable items with you when not in your hotel room.

In the counterintelligence world there are no coincidences. Because elicitation and searches are subtle and difficult to recognize, report any suspicious conversations or activities to your local counterintelligence or security office.

ARTICLE SUBMISSIONS AND READER FEEDBACK WELCOME!

Counterintelligence Quarterly:
Reporting on the nexus between
quality science, technology and
counterintelligence

Published by:

U.S. Department of Energy
Office of Counterintelligence
1000 Independence Avenue, SW
Washington, DC 20585

Managing Editor:

Jenna McCarthy
Phone (202) 586-4982
Fax (202) 586-0551
email: ciquarterly@cn.doe.gov

LOCAL COUNTERINTELLIGENCE OFFICE CONTACT INFORMATION

Office of Counterintelligence
Richland Regional Office

Contact Us:

By Phone: 373-1865

By E-mail:
^OCINWREGION or
OCINWREGION@rl.gov