HANDOUT 10.1: SAMPLE THREAT ANALYSIS STATEMENT CASE STUDY

Purpose: To examine a sample threat analysis statement in a given case study
Duration: 30 minutes (20-reading; 10-discussion)
Group composition: Table groups
Debrief: Large-group discussion

Directions:

1. Read the sample threat analysis statement and then the case study involving the South African nuclear power facility.
2. Discuss the questions about the case study with your group.
3. Write your responses to the questions in the spaces provided.
4. Be prepared to share your answers with the class.

Sample Threat Analysis Statement: Nuclear Power Facility

The following example is part of an outdated threat analysis statement used by a nuclear power facility in South Africa. The facility:

- Categorized each threat by group
- Did not consider theft of material for financial gain by a criminal a viable threat
- Did not include this type of theft in their threat analysis

Terrorist (Radiological Sabotage)

A determined violent external assault, attack by stealth, or deceptive actions, including diversionary actions, by an adversary force capable of operating in each of the following modes:

- A single group attacking through one entry point
- Multiple groups attacking through multiple entry points
- A combination of one or more groups and one or more individuals attacking through multiple entry points
- Individuals attacking through separate entry points

Operating with the following attributes, assistance, and equipment:

- Well-trained individuals
  - Dedicated and willing to kill or be killed
  - Military training and skills
  - With sufficient knowledge to identify specific equipment or locations necessary for a successful attack
- Active insider
  - Facilitate entrance and exit
  - Disable alarms and communications

  - Participate in violent attack
  - May be working with passive insider
- Passive insider
  - Provide information
  - Knowledgeable inside assistance
  - May be working with active insider
- Suitable weapons, including handheld automatic weapons
  - Equipped with silencers
  - Having effective long range accuracy
- Hand-carried equipment, including incapacitating agents and explosives
  - For use as tools of entry
  - For otherwise destroying reactor, facility, transporter, or container integrity or features of the safeguards system
- Land and water vehicles
  - For transporting personnel and their hand-carried equipment to the proximity of vital areas
  - An internal threat
  - A land vehicle bomb assault (may be coordinated with external assault)
  - A waterborne vehicle bomb assault, which may be coordinated with an external assault
  - A cyberattack

Terrorist (Theft or Diversion of Formula Quantities of Strategic Special Nuclear Material)

A determined violent external assault, attack by stealth, or deceptive actions, including diversionary actions, by an adversary force capable of operating in each of the following modes:

- A single group attacking through one entry point
- Multiple groups attacking through one or more entry points
- One or more individuals attacking through multiple entry points
- Individuals attacking through separate entry points

Operating with the following attributes, assistance, and equipment:

- Well-trained individuals
  - Dedicated and willing to kill or be killed
  - Military training and skills
  - With sufficient knowledge to identify specific equipment or locations necessary for a successful attack
- Active insider
  - Facilitate entrance and exit
  - Disable alarms and communications
  - Participate in violent attack
  - May be working with passive insider

- Passive insider
  - Provide information
  - Knowledgeable inside assistance
  - May be working with active insider
- Suitable weapons, including handheld automatic weapons
  - Equipped with silencers
  - Having effective long range accuracy
- Hand-carried equipment, including incapacitating agents and explosives
  - For use as tools of entry
  - For otherwise destroying reactor, facility, transporter, or container integrity or features of the safeguards system
- Land and water vehicles
  - For transporting personnel and their hand-carried equipment to the proximity of vital areas
  - An internal threat
  - A land vehicle bomb assault (may be coordinated with external assault)
  - A waterborne vehicle bomb assault, which may be coordinated with an external assault
  - A cyberattack

Nuclear Power Plant Attack Case Study — Pelindaba, South Africa

The November 9, 2007, attack at the Pelindaba, South Africa, nuclear power plant is an excellent example of the need for a threat analysis. As relayed by eyewitnesses four armed gunmen entered the Emergency Control Room of the facility. The men had apparently:

- Breached an electrified fence (10,000 volts)
- Circumvented the security closed-circuit television units
- Walked approximately 1.2 kilometers to the Emergency Control Room

Once inside the Emergency Control Room, a male employee of the facility confronted the gunmen. A fight followed, which left the male employee injured and incapacitated. The male employee was able to call the Security Control Center to report the attack before the gunmen attacked him. The gunmen assaulted a second employee (a woman) in the Emergency Control Room and held her captive during the assault on the facility. During this time, others reported that a second group of gunmen attempted to cut through the fence. During their breach attempt, the gunmen exchanged gunfire with one of the security force members. This second group retreated and therefore failed to enter the facility.

The attackers' tactics included:

- Breaching an electrified perimeter fence
- Disabling the electric fence once inside the perimeter
- Disabling the tamper sensor device, which was designed to notify the security control center in the event of an intruder's attempts to disable the electric fence control box
- Traversing 1.2 kilometers to the Emergency Control Room
- Breaking into the Emergency Control Room and attacking the operators

Unclear on what motivated the two groups of attackers to depart, the adversaries in the Emergency Control Room and the other adversary group attempting to breach the fence left the facility. Although there is considerable debate about which asset the attackers were seeking, security experts are assuming that the target was the weapons-grade uranium stored at the facility.

Investigation efforts have yet to provide additional information about the incident, but the following facts are known:

- The Emergency Control Room operator that was scheduled to be on-duty the evening of the attack called in sick, which caused investigators to believe that the operator was aware that something was going to happen that evening.
- The security force took 24 minutes to respond to the Emergency Control Room.
- Two closed-circuit television operators were fired due to their failure to observe the intruders.

Government officials refer to the Pelindaba facility as a "national crucial point;" this means the government considers the facility to be a critical infrastructure.

1. **What critical information was not included in the sample threat analysis?**

2. **What were some of the significant points of the case study?**

3. **What were some of the security countermeasure failures?**

This Page Intentionally Left Blank.