WORKBOOK 10.2: INSIDER THREAT WORKSHEET ACTIVITY

Purpose: To provide a template and an example to help organize gathered information about insider threats
Duration: 15 minutes (5-reading; 10-discussion)
Group composition: Table groups
Debrief: Large-group discussion

Part 1: Insider Threat Information Worksheet Example

Recall that insiders have special knowledge, access, and opportunity. Consequently, insiders represent a unique threat to a critical infrastructure facility. Your threat analysis begins by looking specifically at the potential threats presented by insiders. Here is a sample template to help you organize information.

In the example below, a senior facility manager received a medium rating under the **Access to asset** column. The basis of this rating may be the fact that although this individual has access to the asset, he or she may not visit the critical infrastructure facility often. Review the sample worksheet and then review the threat information details below.

Table 1: Sample Insider Threat Information Worksheet

Threat opportunity → / Insider categories ↓	Access to asset	Access to physical protection system	Knowledge of security	Theft opportunity	Sabotage opportunity	Conspiring opportunity
Senior facility manager	Medium	Low	Low	Low	Low	High
Control operators						
Maintenance personnel						
Security force managers						
Security force personnel						
Other:						

Once completed, this worksheet will allow you visualize the threat from each insider adversary category. The more **High** appears in each category, the greater the potential threat to the facility. The rationale for your decisions to rate each category of insider should be logical.

For demonstration purposes only, the following threat information is the basis of the logic behind rating the senior facility management received (collected from facility personnel interviews):

- The senior facility manager does have access to the asset, but more than likely a subordinate would accompany the manager when in the asset area.
- The senior facility manager does not have direct access to the physical protection systems and if he or she requested such information, it would draw suspicion among subordinates.
- Knowledge of security force activities would be limited, because the senior facility manager does not have a need-to-know and if he or she asked questions, it would again draw suspicion from subordinates.
- Theft and sabotage for this category of individual would also be low for the same reasons as stated, but opportunity for conspiring is high, because the individual has the authority to request access to the area based on his or her position and could allow an outsider direct access.

Part 2: Completed Insider Threat Information Worksheet

Once the insider information worksheet is completed, you can determine which insider category presents the highest probability of a threat. When designing the physical protection system, it will be important to identify mitigating factors to help prevent the insider threat. Such mitigating factors might include:

- Requiring comprehensive background investigations
- Restricting access to sensitive areas
- Requiring people to work in pairs around sensitive assets

You will complete *Table 2: Completed Example Insider Threat Information Worksheet* as a group and your facilitator will present the logic for the possibilities to complete the table. Write the possible ratings in the boxes in Table 2.

Table 2: Completed Example Insider Threat Information Worksheet

Threat opportunity → **Insider categories ↓**	**Access to asset**	**Access to physical protection system**	**Knowledge of security**	**Theft opportunity**	**Sabotage opportunity**	**Conspiring opportunity**
Senior facility manager	Medium	Low	Low	Low	Low	High
Control operators						
Maintenance personnel						
Security force managers						
Security force personnel						
Other: *Participants may add other categories*						

This Page Intentionally Left Blank.