24. Insider Analysis

Abstract. The term "insider" describes one or more individuals with authorized access to nuclear facilities or nuclear material in transport who could attempt unauthorized removal or sabotage, or who could aid an external adversary to do so. Facilities handling nuclear materials and other attractive targets should consider the possibility of malicious action by an insider. The insider has unique capabilities compared to the "outsider" adversary, such as authorized access, authority, and knowledge. Insiders may also act in collusion with outsiders. Prevention and protection against the insider threat includes identifying facility-specific insider groups, using a system approach to design relevant preventive and protective measures, and analyzing, evaluating and improving protection system effectiveness.

24.1 Introduction

Insiders Have Access, Authority, and Knowledge, An insider adversary could be anyone who has authorized access to the facility, regardless of position of authority or level of knowledge. Insiders present a unique problem for a physical protection system. Insiders could take advantage of their access, complemented by their authority and facility knowledge, to bypass protection elements, including safety, material control and accountability, and operating measures and procedures, and to entry control systems to perform acts of sabotage or unauthorized removal. Further, as a trusted person, the insider is capable of using defeat methods not available to outsiders when confronted with protection elements and entry controls. The insider can select the most vulnerable target, the best time to execute the malicious act, and can stretch the malicious act over a long period of time if it increases the likelihood of success. This could include, among other things, modifying safety equipment or stealing small amounts of material over an extended period.

Insider Categories

Insiders may be passive or active, violent or nonviolent, internally motivated or externally coerced (see Figure 24-1).

- The passive insider is nonviolent, limiting his participation to providing information about facility operations and safeguards to a colluding insider or outsider(s). The passive insider provides only the information that he or she can readily obtain and divulge without fear of detection.
• The **active insider** is willing to provide information, perform actions for the adversaries, and may be violent or nonviolent. The active insider is willing to open doors and provide hands-on help; and may even aid in neutralizing response force personnel.

  – The **nonviolent active insider** is not willing to be identified or risk the chance of engaging response forces and may limit his or her activities to tampering with security systems or operations control systems.

  – **Violent** active insiders may use force regardless of whether it enhances their chances for success or not. The violent insider may be psychotic, a criminal or a terrorist.

Types of Insiders

Types of insiders include criminals, disgruntled employees, ideologues, and psychotic individuals.

• The **criminal insider** may have a prior history of committing criminal acts. Every day, U.S. businesses lose 70 million dollars to theft, and in the year 2000 employee theft accounted for 44% of these losses. The insider criminal is a very real threat.

• Typically, the **disgruntled employee** is a person who has been employed in their position for several years, but who has become dissatisfied with the working environment. Another employee may be happy with the job, but external influences could cause the employee to act inappropriately at work. The most common cause in these situations is an unhappy domestic life. Employees might be worried about possible layoffs or increased workloads, which could raise stress levels and cause actions against management. Other employee-related problems can include drug abuse and a wide range of psychological problems such as long-term depression.

• Some insiders are motivated by **ideological beliefs**, such as anti-nuclear activists, who believe so strongly in certain issues that they are willing to defy the law for the sake of their beliefs. These insiders are typically bright individuals who have a committed attitude and a rebellious nature.

24.2 Past Incidents

Analysis of past insider incidents indicates that insiders are among the most difficult threats to defend against. In a study of commercial industry incidents, members of the security force represented approximately 41% of insiders who commit acts against the facilities. No similar conclusions can be drawn from the limited data available for the nuclear industry. However, the response force is probably one of the very few groups of individuals that have complete access to any place within the protected area and would not attract any suspicion based on their presence. In addition, they are often some of the lowest-paid employees.

**Examples of Insiders Are Difficult to Defend Against**

In December 1987, an American PSA Flight 1771 crashed and killed everyone...
Disgruntled Employees

one aboard. The perpetrator was a former employee who had been fired from the airline for alleged misconduct. Although no longer an employee of the airline, he was able to use his access card to gain entry into the plane with a gun in his possession. Once in the air, the ex-employee gained control of the cockpit and shot the crew. Shortly after the incident, the Director of Security for the Federal Aviation Administration (FAA) was quoted, “The most difficult problem (in personnel screening at airports) is those with knowledge and access” (Associated Press, 1987).

An example of a computer-related incident involving a disgruntled employee took place in September 1996. A small Internet provider was virtually destroyed by the former employee who, on the day he was laid off from his job, accessed the company’s files and erased all the data and back-up files (USA Today, 1997).

On December 4, 1997, staff at McGuire Nuclear Station, Unit 2 discovered indications of potential tampering with the upper and lower personnel air lock seals. The air lock design incorporates two inflatable seals per door, for a total of four seals per air lock. The damage was identified during the performance of required testing of the air lock seal integrity to support restart of the unit. A sharp instrument was used to damage the seals. The plant staff determined that all of the eight seals had been cut. No additional indications of tampering were identified. Walkdowns of plant systems conducted before this tampering event also identified mispositioned valves. The unit was shut down to replace the steam generators and undertake refueling at that time. The utility speculated that the tampering might have been related to a work-force-reduction announcement.

Attempted Extortion by Temporary Employee

On Friday, January 26, 1979, a temporary employee of subcontractor working at the General Electric low enriched fuel fabrication plant in Wilmington, North Carolina, stole two 5-gallon containers of low enriched UO₂ (~145 pounds total). The theft was accomplished as follows. After working the day shift, he drove back to the plant at 10:50 p.m. and entered with the night shift. He circumvented the entry controls at the entrance gate by showing the guard his Florida driver’s license which looked similar to a picture badge authorizing access to the plant area where the UO₂ was processed. His yellow contractor badge would not have permitted access to this area. He had allegedly used his driver’s license to gain access to this area on previous occasions. Once inside the plant, the subject would have been guided by gates and fences into a parking area had it not been for the fact that one gate had been removed to allow installation of truck scales. The missing gate made it possible for him to drive to an area adjacent to the building he wanted to enter and park his car. He entered the building and went to his normal workstation, the Chem Tech Lab, entering it using his key. In the lab he picked up his protective clothing, a two-wheel cart used to move 55-gallon drums, and a container used to ship chemicals. The container could hold two 5-gallon cans. He then proceeded to a door leading up a stairwell into the radiation controlled area. The door was normally locked (though there was no regulatory requirement to do so). However, at this time it was slightly ajar due to malfunction of the locking mechanism. Once through the door, he put on his protective clothing and
went up the stairs to the Blend Queue Area. He removed two 5-gallon cans of UO₂, carried them down the stairs and put them in the shipping container. He then removed his protective clothing and retraced his steps back to his workstation, the Chem Tech Lab.

Once back in the lab he opened one can and removed some of the material, which he intended to use to affect his blackmail scheme. Using the two-wheel cart, he transported the remaining material to his car and loaded it into his trunk. He retraced his steps and left the plant just before midnight on Friday, January 26. (Plant procedures required anyone leaving the plant after midnight to sign out.) He had been in the plant approximately one hour. He had entered the plant with the incoming plant change and had left with the outgoing shift.

At 11:45 a.m. on the following Monday, January 29, the plant General Manager reported to authorities that he had found an extortion letter and a sample of UO₂ at his door when he came to work. The letter stated that the writer had taken two 5-gallon containers of UO₂ from the plant and identified the containers by serial number and gross weight. The letter also stated that sufficient UO₂ had been removed from one of the containers to furnish samples to newspaper editors, Senators, anti-nuclear group leaders, and others if his demand for $100,000 in cash was not met by Thursday, February 1. The writer further threatened that, after the samples had been delivered, if he had not received the money, one container of UO₂ would be dispersed through one unnamed large American city. The UO₂ powder from the second container would be dispersed through another large city if an additional $100,000 was not provided at that time.

As the General Manager was in the process of verifying the authenticity of the container numbers and determining whether they were missing, he received independent notification from the plant near-real-time accounting system that the two containers were not in their assigned locations and could not be accounted for. The Federal Bureau of Investigation (FBI) assumed investigative jurisdiction on January 29 and arrested the perpetrator on February 1, 1979. The perpetrator, a temporary employee, was subsequently convicted and sentenced to 15 years in prison. (From IE Circular No. 79-08, “Attempted Extortion – Low Enriched Uranium,” May 17, 1979.)

In August 1992, a 7-meter-long fuel assembly weighing 270 kg and containing 111 kg of 2% enriched LEU was stolen from the Ignalina Nuclear Power Plant, in Ignalina, Lithuania. It was removed from the facility by attaching it to the bottom of a duty bus. The investigation revealed that the reactor operation personnel and the guards had carried out the theft. About 80 kg of the stolen LEU are said to have been recovered on several occasions between 1992 and 2002. (Presentation by Chaim Braun, Fritz Steinhausler, and Lyudmila Zaitseva at the ANS 2002 Winter Meeting.)

In 1992, Russian security agents detained a group of criminals who had been stealing Uranium from the Chepetsk plant in Izhevsk and seized 140
24. Insider Analysis

kg of LEU (2% to 4% enrichment). Facility employees stole the material taking advantage of an accounting system weakness that allowed a 4% “loss of inventory” in material balance closures. Based on the incident, an inventory was conducted at the plant and 300 kg were found to be missing. Parts of the diverted material are believed to have been seized in Poland, Belarus, Lithuania, Russia, and Chechnya between 1992 and 2002. (Presentation by Chaim Braun, Fritz Steinhausler, and Lyudmila Zaitseva at the ANS 2002 Winter Meeting.)

24.3 Opportunity, Motivation, and Attempts

**Opportunity**
The combination of access, authority, and knowledge combine to provide the insider with an opportunity to commit a malicious act.

- **Access**: Insiders by definition have authorized access to work areas in a facility. They may also have special temporary access, including emergency access by fire, medical, or police responders. They may be escorted or unescorted, and may have other restrictions during access. Because of their knowledge or authority, they may be able to obtain unauthorized access to certain areas. They may have access to protection equipment, process tools, or other special site equipment that they could exploit. They may also know about and gain access to target material during vulnerable conditions of sufficient duration to perform malicious acts.

- **Authority**: Insider authority may be over personnel, such as designated authority or personal influence, or over tasks and equipment, such as alarm assessment, sensitive documents, or authorization for processes and procedures.

- **Knowledge**: Insider knowledge may comprise target information, security system details, or information about site tools and equipment. Target information includes locations, characteristics, durations, and other details of targets, as well as details of facility layouts. Security system information includes response force capabilities and communications, details of facility and security operations, as well as the location and operational details of safety equipment.

**Motivation**
Insider motivation may be ideological, financial, revenge, ego, mental stability, or coercion. Motivation is an important indicator for both level of malevolence and likelihood of attempt.

**Insider Advantages**
- **Unique capabilities**: Insiders can select the best time and strategy to be successful in their task. Because of their unique capabilities, they can exploit time, tools, tests, and collusion to be successful.

- **Time**: Insiders can select the optimum time to implement a plan, and they can extend acts over long periods of time to avoid detection.

- **Tools**: Insiders have the capability to use tools located at work stations, or to introduce contraband tools into the facility.
• **Tests:** Insiders can test the protection system with intentional, normal-looking “mistakes.”

• **Collusion:** Insiders may recruit, direct, coerce, or collude with others, including both other insiders and outsiders.

**Attempts**

The combination of access, authority, and knowledge attributes may provide an insider with an opportunity for the commission of a malicious act. Opportunity, when combined with motivation, may lead to an actual attempt to commit a malicious act. The system to prevent and protect against insiders is predicated on this combination of opportunity and motivation.

### 24.4 Measures to Prevent and Protect Against Insiders

**General Approach**

The insider problem must be approached in a different way than that of the outsider. The outsider attacks can only be addressed once they occur but there are several elements of the insider protection system that reduce the likelihood of a malicious insider presence as well as elements that detect and prevent insider malicious actions. The insider protection approach can be broken into several sequential phases, as shown in Figure 24-2. The process to prevent and protect against insiders consists of five steps:

1. Exclude potential insiders from obtaining access,
2. Remove potential insiders after they have access,
3. Minimize opportunities for committing malicious acts,
4. Detect, delay and respond to such acts, and
5. Mitigate consequences from a completed act.

**Figure 24-2. Insider Protection System Approach**

**Personnel Security Programs**

*Personnel Security Programs* contribute in Steps 1 and 2 to exclude and remove potential adversaries, and include:

- initial access authorization (personnel clearances)
- periodic background checks
Physical Security Systems

- security education and awareness (security culture)
- control of visits
- the Human Reliability Program (HRP)

Physical Protection Systems contribute mainly in Steps 3 and 4 to minimize opportunity and to detect, delay and respond to any malicious activities that do occur. These systems include the following:

- barriers and other access delay systems
- intrusion detection systems
- contraband detection
- entry controls to monitor access and exit
- surveillance
- response force
- contingency and emergency plans

Material Control and Accountability

Material control and accountability systems are an important part of both Steps 3 and 4. Physical consolidation of material to reduce the number and location of target material is also important.

24.4.1 Exclude Potential Adversaries with Pre-Employment Checks

Pre-Employment Checks

The first step is to filter potential employees and contractors. A pre-employment investigation is a systematic compilation and evaluation of information collected through inquiries made in person, by telephone, or in writing with the intent to establish the general character, trustworthiness, and reliability of prospective employees and contractors. These investigations are not trivial. In the U.S., they are often done by the FBI and cost more than $10,000 for each investigation.
24.4.2 Remove Potential Adversaries after They begin Activities at the Facility

Develop a Desirable Working and Security Culture
Once a clearance is granted, it should be re-evaluated periodically, for example, every five years. Through a continuing program of security education and awareness, a security culture can be established which tends to minimize malicious activity. The level of employee satisfaction can be enhanced by good working conditions, well-conducted training, and employee benefits (insurance, holidays, etc.). Operational quality control programs also assist in reducing the motivation and opportunity for malevolence. Finally, special programs for those few individuals who have direct access to critical areas can be put into place. In the U.S., one of these is called the Human Reliability Program (HRP). Many facilities worldwide also have “fitness for duty” requirements. All of these programs are intended to reduce the number of potential insider adversaries. If disciplinary action is invoked when malevolence occurs, additional malicious activities may be deterred.

Educate Employees
Security awareness is an integral element for physical protection systems. Employees are required to attend briefings that apply to their specific access needs. The goal of the security education program is to inform the employees of their security responsibilities, to alert them to actual or potential threats, and to motivate them to maintain a high level of security awareness.

Types of Briefings
In the U.S., several types of briefings are used in the Security Education and Awareness Program. Examples include:

- Initial Briefing,
- Comprehensive Briefing,
- Annual Refresher Briefing, and
- Termination Briefing.

Information Contained in Briefings
These briefings typically incorporate the following information:

- applicable Security directives and procedures,
- site-specific (and/or operations-specific) security policies, procedures, and requirements,
- recent espionage cases,
- approaches and recruitment techniques employed by foreign intelligence services,
- security incidents and considerations, and
- security threats and vulnerabilities.

New Employees
The Initial Briefing is provided to individuals approved for unescorted
Receive an Initial Briefing

access to security areas and is included as a module in new employee training. Briefing topics may include:

- an overview of security disciplines, such as personnel security, information security, and physical security
- local entry control procedures and escort requirements
- protection of property
- prohibited articles
- reporting incidents of a Security concern

Topics for Comprehensive Briefing

The Comprehensive Briefing is provided to individuals before being granted access to classified information or to special nuclear material (CATEGORY 1). An employee receives a Comprehensive Briefing after their security clearance has been granted. A Comprehensive Briefing is provided before receiving a cleared security photo badge.

Comprehensive briefing topics could include:

- information security
- physical security
- personnel security
- reporting/notification requirements
- legal and administration sanctions imposed for incurring a security infraction or committing a violation
- general information concerning the protection of CATEGORY 1

Annual Reminders

The Annual Security Refresher Briefing is provided annually to cleared employees. The briefing reminds employees of their security responsibilities and outlines updated security policies.

Termination Briefing Describes Post-Job Responsibilities

The Termination Briefing is provided to individuals who are terminating their security clearance. The Termination Briefing is provided on the last day of employment, the last day an individual possesses a security clearance, or the day it becomes known that the individual no longer requires access to classified information or CATEGORY 1, whichever is sooner. A Termination Statement is provided to the employee when the cleared security badge is returned to the facility. This briefing clearly explains the person’s status (uncleared) and the ongoing responsibility not to divulge important information and data.

HRP Applies to Certain Employees

The Human Reliability Program (HRP) is a continuous evaluation program for individuals who:

- have direct access to, protect, or transport Category I quantities of CATEGORY 1,
- perform duties as reactor operators, or
- may cause an unacceptable risk to national security.

HRP Activities

Continuous evaluation is accomplished through initial assessment and recurring assessments consisting of supervisory reviews, medical
assessments, management evaluation, and security determinations. The HRP also includes training for supervisors in how to recognize aberrant behavior. Aberrant behavior is defined as behavior that deviates from normal or typical behavior that is expected from an individual or behavior that is contrary to socially accepted behavior. HRPs provide for testing for controlled substances or the habitual use of alcohol, which may impair judgment, trustworthiness, and reliability.

An effective HRP requires that an organization makes this program mandatory for personnel in key positions. Persons in these positions must complete an initial certification and an annual recertification.

After the initial training has been completed, the applicant receives a HRP Medical Assessment. The applicant must sign a consent form for the HRP. A physician examines the applicant to ensure there are no concerns (such as substance abuse) that indicate that the person might not be trustworthy. This involves:

- a physical examination,
- a random drug screen, and
- a psychological assessment.

The next step in initial certification may be a polygraph examination. The polygraph is limited to the topics of espionage, sabotage, terrorism, intentional unauthorized disclosure of classified information, intentional unauthorized foreign contacts, and deliberate damage or malicious misuse of government property or a defense system. Controls are in place to prevent unwarranted intrusion into the privacy of individuals. Questions will not be asked about an individual’s thoughts, beliefs or conduct that has no counterintelligence implications, or no direct relevance to an investigation.

Applicants complete an initial substance abuse test for illegal drugs and alcohol.

Once a person passes these tests, they are enrolled in the Human Reliability Program (HRP).

Annually, all HRP employees have a medical and psychological examination as described above. Random drug tests may occur during the year. A major feature of the HRP is that all supervisors are trained to observe aberrant behavior, and at any indication of the following action must be taken:

- suspicion of excessive alcohol or substance abuse on or off the job,
- psychological or physical disorders that impair performance of assigned duties,
- significant behavioral changes, moodiness, depression, or other evidence of loss of emotional control (i.e., crying bouts, uncontrollable anger),
• inability to deal with stress or the appearance of being under stress,
• hostility or aggression toward fellow workers or authority,
• evidence of a pattern of poor decision making or irresponsibility, or
• failure to follow direct orders or a violation of safety, security, or work procedures.

OPSEC programs are developed to limit the information available to those without a need-to-know. This information can be unclassified, sensitive, or classified information that on its own may not assist an insider in planning or executing an attack, but when taken in conjunction with other information, completes a “puzzle” and provides essential information to potential insiders. With an effective OPSEC program, this essential information can be identified and properly protected in order to limit the number of people who have the “high degree” of knowledge that would make a dangerous insider.

24.4.3 Minimize Opportunities for Malicious Activities

Access Authorization
Access authorization is the process of determining eligibility for access. Access can be granted to sensitive information and facilities if the individual meets the requirements for obtaining a security clearance through pre-employment screening and background investigations.

Badges Provide Identification of the Person and Clearance Level
Once a person is cleared, they are issued a badge to identify them and their clearance status. These badges are appropriately colored and coded. They are used and accepted as evidence of an access authorization (or security clearance level). Some sites may require presentation of additional photo identification or further positive personnel identification.

Keep Badges Up to Date
Badges are to be worn conspicuously, photo side out, in a location above the waist and on the front of the body while at the facility. The badges must be maintained in good condition. If a significant change in appearance takes place, such as facial hair, new glasses, and so on, the individual must obtain a new badge with a new photograph. Guard force personnel are authorized to confiscate faded, worn, or damaged badges.

Keep Records of Badges and Maintain a Database
Badge inventories and records are maintained. Such records include, at a minimum: description and serial number of item issued, date of issuance, name and organization of holder, and date of destruction. A record of missing badges and credentials is also maintained. Personnel and/or systems controlling access to security areas are given current information regarding missing badges in order to prevent their misuse. The loss of badges must be reported immediately.

Escorting Visitors
Visitor control procedures ensure that only appropriately cleared individuals gain access to security areas and facilities. Unescorted access onto the site and into the facilities is granted to employees and contractor personnel who have an authorized photo badge. Unescorted access onto the site and into buildings may be granted to visitors or employees with a one-day pass or temporary badge. Visitors must be escorted upon entry to sensitive areas.
Responsibilities of Escorts

Escorts must be knowledgeable of security plan requirements and they must:

- be familiar with areas the escorted person is to visit and also be aware of precautions necessary to prevent unauthorized access to classified matter or special nuclear material,
- be aware of the scope of work the visitor is to perform, and familiar enough with the work to be performed to notice if non-authorized activities are taking place,
- not deviate from the exact route when routes are specified,
- not delegate responsibilities to another person unless prior arrangements have been made with appropriate personnel,
- discuss only authorized information,
- not admit visitors to any area or building unless such access is indicated on the visitor’s badge or authorized by appropriate security personnel,
- ensure that personnel being escorted are aware of all security rules and procedures,
- ensure that personnel being escorted remain within sight and normal voice communication at all times,
- maintain a knowledge of escort security plans,
- be thoroughly familiar with the security rules and procedures of the area in which they are performing escort duties,
- where required, properly sign in the persons being escorted before entering security areas, and
- notify security personnel when problems occur.

Responsibilities of Facility Personnel When Visitors Are Present

Persons assigned to the facility to be visited (and responsible for the visitor) must:

- ensure that the visitor has an authorized visitor’s badge, where required,
- ensure that the visitor is escorted at all times during the visit while they are inside the facility, and
- ensure that the visitor is not allowed access to classified or sensitive information or equipment, unless the visitor is cleared to the appropriate level and has a “need to know” in the performance of their official duties.

Reduce Number of People with Access

In the design of the facility, special care is taken to reduce the opportunities that workers have for theft or sabotage. Insider direct access to sensitive equipment and nuclear materials must be limited to those who must have access to perform their jobs and must be limited to the periods necessary for performance of duties. Entry control systems provide the capability to restrict access to sensitive areas and materials to only those who have been previously authorized for such access. This approach reduces the number of insiders who can commit malicious acts in these areas.

Material Consolidation

Material consolidation and inventory reduction can also assist in reducing the theft attempt possibilities of the insider. One measure is to place all CATEGORY 1 in central locations and keep on hand only the amount that
is actually needed. The remainder is shipped to a centralized repository.

Automated systems require significant pre-planning to ensure that when people arrive at a location to do a critical job, they are scheduled to do the job and are the appropriate people to do it. Making and keeping accurate daily schedules and plans is a significant deterrent to an insider who might depend on confusion and mismanagement to mask his activities.

Strict Procedures

Deter Insiders with Fear of Being Caught

Although physical security measures are used to limit access and to detect and delay intruders, they can also provide deterrence if the insider believes there is a high probability of being caught due to the physical security measures in place. Physical security can include barriers, intrusion detection systems, contraband detection, entry controls, surveillance, response, and contingency plans.

Compartmentalize the Facility to Prevent Access

To maximize the effectiveness of an internal entry control system, the facility must be compartmentalized to prevent access by people who are not authorized to handle CATEGORY 1. Often older facilities were designed with efficiency of operation in mind (open rooms with smooth flow of process material) and this makes physical security against the insider threat much more difficult. A facility should be segmented and compartmentalized as much as possible. Then, access should be carefully controlled in each compartment of the facility to make sure that only the authorized people at the authorized time enter those areas and that they do only authorized activities. Having such careful control within a facility will minimize malicious attempts because the risk of detection is too high and chance of escape with the material is too low for an insider to attempt a theft.

Closely Monitor Vital Equipment Operations

Knowledgeable oversight of the specific details associated with maintaining and calibrating sensitive equipment minimizes the opportunity for maintenance personnel to commit malicious acts during the regular course of their duties.

Nuclear Safety and Facility Design

The nuclear safety requirements and the subsequent design of facilities also provide additional measures that tend to preclude insider opportunities.

Quality Assurance

A quality assurance program contributes to the protection against insiders by establishing an environment where work planning and control are essential to performance of duties. In work planning, functional roles, levels of authority, and work interfaces are defined and documented. Control consists in part of ongoing assessments of work activities to determine if work is being performed in accordance with established procedures and processes. A formal QA program will help deter an insider, and by strictly defining the work process, can minimize insider opportunities.

24.4.4 Detect, Delay and Respond to Malicious Action

Two-Person Rule | The “Two-Person Rule” is used to minimize opportunities for malevolence
and detect malicious acts when they occur. In places where one person could easily have access to CATEGORY 1 or vital equipment, there needs to be an enforceable administrative process to ensure that any person cannot be in that location or do that job without another person present. The two people must remain in full view of each other at all times and must be equally qualified so that each will be able to recognize if the other is performing an unauthorized activity. This process can be enforced manually by posting a guard at a door allowing entry only if the proper two people are present. Automated methods of enforcing this rule with entry control systems can ensure automatically that the door to the area will not open unless the authenticated credentials of two qualified workers are presented.

Control of personnel in some very sensitive areas may be enhanced even further by sensors in rooms that can record the exact location of each badge and each target item within the room. There are technologies to ensure that a badge is actually attached to the proper person (e.g. a fiber optic link around the wrist or around the neck) and therefore the person’s location can be verified. The system is then programmed with the locations that each person is authorized to be in, and the distance that personnel can be apart and still be able to monitor the activity of the other. If any of the parameters are exceeded, an alarm is sounded and the guard force will investigate the infraction. The data from the location sensors and the data from the door sensors are kept in a secure database, and if unauthorized activity is suspected the tracking data can be reviewed to make a list of potential suspects.

Supervisors are not only supposed to watch the employees for changes in their behavior, but supervisory review of all operations is essential to good protection against the insider threat. A supervisor knows who should be in what areas and how long they should be there, and if anything unusual is happening the supervisor should be able to identify the problem. This, of course, raises the issue of “who watches the supervisor?” because the supervisor could be the insider. Every supervisor has a supervisor and the chain of command watches the people under their control.

Entry and exit points to Material Access Areas should be minimized, and searches should be conducted at entry and exit points to ensure that contraband is not introduced into the area, and that material is not removed from the area.

Metal detectors and X-ray machines should be installed at the entrance to areas where insiders should not bring contraband (weapons, etc.). At the exits from Material Access Areas, install metal detectors and CATEGORY 1 detectors through which all personnel must pass. The CATEGORY 1 detector is usually a portal device that is set as sensitively as possible, given the background radiation of the area. Sometimes a timer is required to keep the employees standing in the counter until a statistically significant count is obtained and it is determined that the person is not carrying CATEGORY 1. A guard force person should be posted to ensure that procedures are followed and to respond if a theft attempt is detected. A metal detector is
used in conjunction with an CATEGORY 1 detector because the insider could carry the CATEGORY 1 in a shielded container. The metal detector would alarm if a shielded container were being carried out of the area.

Some of the protection systems employed within a facility (such as the alarm system) might be an initial target for an insider. Supervision techniques should be used for the physical protection signal wires to ensure that no insider can tamper with or deactivate protection systems. All lines that transmit alarms and physical protection data are supervised either by using direct current (DC) line supervision or a more elaborate active interrogation system. If an insider attempts to deactivate the alarm system to either mask his activities or to assist an outsider to enter the facility without being detected, the supervisory systems would cause an alarm. Fiber optic transmission systems increase the difficulty of the adversary tampering with the signal lines without detection.

Similarly, procedures should be in place to ensure that personnel authorized to work on the protection systems cannot use this authority to tamper with the systems. The Two-person rule and systems of independent tests can be used to provide this type of tamper protection.

Many of the sensors used to detect unauthorized insider activity inside the facility have a self-test feature. This enables the sensor to test its ability to detect from the sensor all the way to the alarm station, and any problems or inoperative equipment will be immediately identified. These self-tests are generally conducted automatically by the computer control system of the alarm system and can detect malicious insider actions performed against the security system in preparation for a theft or sabotage attempt.

Another detection/protection measure is material control and accounting programs. These programs detect losses of material, removal of material from authorized storage locations, or other malicious acts and provide an audit trail to detect the responsible parties.

Finally, one area that is often neglected, and that should be monitored by the security personnel is the spare part inventory for the security and vital equipment. If an adversary were able to obtain unlimited access to a spare sensor or pump that would be used to replace another sensor or pump, then internal modifications could be made to allow the adversary undetected access if the spare part were used. The equipment that is critical to the operation of the security system and the spare parts must be protected from tampering by an insider.

Many on the access delay features of the PPS will not delay an insider, because in many cases, the insider has authorized access to target areas, or to the areas immediately surrounding the target areas. There are several ways that delay features can be used to provide delay, even to insiders. Using systems that require two-person input to access material can keep delay in place for insiders by ensuring that two people (from different organizations) are required to open vaults or work areas.
Intimate, or close to the target delay can be used within target areas to further restrict access to material. Material cages, bird-cages, tie-down systems, lockboxes, or other systems can be used to limit and delay access to material. Procedures can also be put in place to limit the amount of material that can be accessed at any given time. This can add complexity and delay to the insider task of acquiring a goal quantity of material.

Separation of duties and use of multi-step processes where no one person accomplishes all of the required process tasks also provides access delay. Breaks in processes for material verification can provide prompt detection of insider activities, and may also complicate and add delay to an adversary theft attempt.

Possible scenarios that would minimize insider delay need to be addressed as well. Emergency exits exist in most areas, and are designed to allow rapid egress. Evacuation alarms and procedures are in place in most areas, and are designed to allow rapid egress from facilities. Measures need to be put in place to provide delay to insider activities, while allowing for safe movement of personnel. Evacuation corrals, enforced muster, and search of personnel prior to release are methods used in many instances to provide additional delay against the insider threat.

Response to Insider Activities

Response to insider activities is different from the response to an attack by Outsider adversaries. It is nearly impossible to detect the actions of a passive insider before the fact. Response in this case would include reporting the incident, investigating the incident, prosecuting the insider, determining the extent of damage and mitigating the damage as feasible.

Timely detection and response to active insider actions is achievable. Initial response to the activities of an active, non-violent insider may be as simple as identification of the activity as abnormal by a fellow worker who challenges the insider and reports the abnormal activity to security. If the insider is non-violent, challenge by a co-worker may be sufficient to stop the activities. If not, the co-worker needs to contact the security forces immediately to stop the insider from completing his tasks. If the insider is violent, only armed response will stop him from completing his tasks. Response measures taken to stop an insider must be rapid, since there is often little time remaining between detection and completion of the insider tasks.

If the insider is successful in removing material from the site, response needs to include coordinated efforts with Local Law Enforcement and State Law Enforcement agencies. Measures may be taken to identify and capture the insider and recover the material before it is irretrievably lost. These response actions should be included in contingency plans, coordinated with the responsible agencies and practiced periodically.

In all cases, follow-on response includes investigation of the incident, and prosecution to the full extent of the law. Investigation of the incident will also lead to identification of previously unknown system deficiencies that must be studied and repaired.
24.4.5 Mitigate Consequences of Malicious Acts

Contingency Plans – Theft

Material inventories are performed often and routinely to identify if any material is missing or misplaced. If a missing amount is larger than the reasonably expected measurement error of the instruments, or if an item is discovered missing during a physical inventory of items, then a contingency plan is put into action immediately. This pre-planned operation stops all egress from the facility and tries to locate the missing material. Part of this plan involves coordination with outside forces to locate material that might have already been removed from the plant. These contingency plans are practiced often and kept up to date for two reasons:

1. to ensure that it will be effective if actually needed
2. to make it clear to all employees that if material is missing, a significant operation will ensue until the material is found.

Contingency and Emergency Response Plans – Sabotage

In addition to contingency plans that address malicious actions, all facilities are usually required by their licensing organization to have an emergency response plan for conditions that may result in off-site dispersal and contamination. These are in place to protect the populace in the event of an accident but are also very useful in the event of an insider-initiated sabotage incident. This pre-planned operation initiates events and actions within the operational system to minimize the effect of safety system compromise. Part of this plan includes coordination with outside emergency responders. This emergency response plan is practiced often and is kept up to date for two reasons:

1. to ensure that it will be effective if actually needed, and
2. to make it clear to all employees that there is significant capability to prevent and/or mitigate the consequences of a sabotage act.

Deter Insiders with Major Personal Consequences

It is also clear to the employees that prosecution after finding the stolen material or ascertaining who caused the incident will be swift and punishment will be sure. In the very few cases in the U.S. of nuclear material being stolen from a plant, the perpetrators were caught and sent to jail with a great deal of publicity. Acts of sabotage have been more difficult to ascribe to specific individuals but when investigations have identified a perpetrator, punishment is swift and appropriate. The purpose of these prosecution actions is to help ensure that no insider will attempt to steal the material or will attempt to sabotage the facility.

24.5 Facility-Specific Insider Analysis Methodology

<table>
<thead>
<tr>
<th>Method to Analyze Effectiveness Against Insider Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>The protection system to counter the insider threat must also be evaluated to determine the level of system effectiveness. The path analysis tools discussed elsewhere in this course are used to analyze the outsider probability of interruption ($P_I$), but similar computer-based techniques are not available to analyze the insider probability of detection.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Steps for Insider</th>
</tr>
</thead>
<tbody>
<tr>
<td>The approach to the analysis of the effectiveness of the physical protection service is based on the ability to detect and deter insiders. This involves evaluating the effectiveness of physical protection systems, including personnel protection, access control, and monitoring systems.</td>
</tr>
</tbody>
</table>
system against the insider uses worksheets to guide and document the evaluation. Examples of these worksheets are included in this material. There are six steps in the manual insider analysis and these steps follow the general DEPO process. The steps are

1. Collect facility or transport information
2. Identify targets of interest
3. Define the facility-specific threat (insider groups)
4. Use the system approach for prevention and protection
5. Evaluate the preventive and protective measure
6. Summarize target/threat results

24.5.1 Collect Facility or Transport Information

Information about the nuclear facility’s layout, organization, operations and systems must be gathered in order to properly characterize the potential vulnerabilities of a facility. This includes the physical protection measures, operating conditions, safety systems, material control and accounting, radiation protection measures, emergency procedures and response. In addition, the organizational chart and personnel responsibilities, operational security awareness, process and procedures, and day-to-day execution of duties must be taken into account.

Information about transport must also be gathered. This includes the physical protection measures (e.g., tracking devices, personnel identity verification, written instructions, confidentiality, etc.), routes and schedules, communications, responsibility of those involved in transport, transportation unit and package characteristics, radiation protection and safety measures, emergency procedures during transport, and response plans.

Conditions favorable for insiders should be identified, such as:

- The conditions inside the facility or regarding the transport, including work force, labor issues, industrial relation policies, security culture and awareness, trustworthiness programs, previous workers, etc.
- The conditions outside the facility or regarding the environment of the transport routes, including the general attitude of the community, and whether the surrounding area is urban or rural. The presence of organized groups, such as any discontented or disgruntled faction of the population, should be reviewed and special attention should be paid to possible connections between this population and persons with experience in or access to the nuclear facility.

24.5.2 Identify Targets of Interest

Target identification is an evaluation of what to protect a priori, including nuclear material, areas, components, systems, and functions, without consideration of the difficulty of providing protection.

Consideration should be given to:
• safety analysis and the associated Vital Area Identification analysis as the starting point to identify potential sabotage targets
• categorization of nuclear material as it applies to the physical protection of nuclear material (INFCIRC/225/Rev 4.) to identify unauthorized removal targets.

The identified targets should be ranked based on the gravity of consequences. Since the objectives of either an unauthorized removal of nuclear material or a sabotage of a nuclear facility are of different natures, the protection goals are also different. Although a specific target may be subject to both unauthorized removal and sabotage, the consequences of these two events may be significantly different. Therefore, a ranking for all unauthorized removal targets should be generated, as well as a separate ranking for all sabotage targets. A unique ranking for both unauthorized removal and sabotage targets together is not generally feasible. This ranking will provide basis for implementing graded preventive and protective measures.

**Sabotage Targets**

Identifying sabotage targets at a facility begins by using safety analyses to identify potential accident sequences, which, if they occurred, would have significant radiological consequences for workers, the public, or the environment. An accident sequence is a series of events resulting from one or more initiating events (human error or the failure of one or more components or functions) that put the facility into a degraded situation despite its installed engineered safety systems and mitigation devices. However, sabotage is not considered in a safety scenario and therefore some other maliciously initiated events may also lead to significant radiological consequences. For example, in some cases the simultaneous failure of the redundant equipment of a safety-related system, such as the pumps of an emergency cooling system, is not considered probable in the safety analysis, yet this failure can credibly be caused by an act of sabotage and can lead to an act with radiological consequences. Components, systems, or functions that could lead to a degraded situation if they were lost or caused to fail by a malicious action must be identified.

The levels of unacceptable radiological consequences are established by the State or the competent authority mainly from the results of safety analysis studies. These consequence levels may vary from State to State. It is desirable that the consequence levels used for malicious incidents consider those taken from the safety criteria. But levels of unacceptable consequences for malicious acts could differ from those considered in the facility safety analysis and may need to be graded in levels below or above those of the safety analysis.

This approach enables the identification of the most sensitive elements in the facility (components, systems, or functions) and their locations, and suggests ranking the targets in categories according to sensitivity. Figure 24-3 illustrates the identification of vital area sabotage targets. Figure 24-4 illustrates the identification of unauthorized removal targets.
24.5.3 Define the Facility-Specific Threat

The State Design Basis Threat (DBT) is the starting point for a facility-specific insider definition. The State DBT for insiders may or may not be detailed. Information for a facility or transport insider analysis should be collected to describe every individual employee or type of potential insider based on levels of access, authority over others, knowledge of the facility operations and other general capabilities that support opportunity for malevolence. Organization charts and job descriptions should be used to determine the levels of access, authority, and knowledge possessed by those engaged in activities at the facility or in the transport. One-on-one discussions and interviews should be conducted with personnel working at the facility or transport to confirm or better understand the levels of access, authority, and knowledge they have.
Other facility or transport characteristics affecting the insider threat attributes should be collected, such as personnel flow and entry control, facility state (normal operation, shutdown, maintenance duty, etc.), operational processes, authority structure, general job categories, physical protection features, information characterization, safety and/or radiation protection requirements, and accountancy and control systems for nuclear material.

In addition to potential insiders identified through their authorized access, specific consideration should be given to people with no access to a facility but with sufficient knowledge and/or authority to conduct a malicious act.

This large list of potential insiders may be impractical. Since many types of potential insiders may have similar or identical attributes, insider types should be grouped. The grouping should then result in a concise, credible but comprehensive list of insider groups. Figure 24-5 illustrates how the complete list of potential insiders for a facility may be grouped.

Facility Personnel Category

<table>
<thead>
<tr>
<th></th>
<th>Facility Personnel Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>Patrol Guards</td>
</tr>
<tr>
<td>17</td>
<td>Post Guards</td>
</tr>
<tr>
<td>18</td>
<td>Janitorial Staff</td>
</tr>
<tr>
<td>19</td>
<td>Material Balance Area Custodians</td>
</tr>
<tr>
<td>20</td>
<td>Nuclear Material Technicians</td>
</tr>
<tr>
<td>21</td>
<td>Nuclear Material Accountability Technicians</td>
</tr>
<tr>
<td>22</td>
<td>Engineering Support</td>
</tr>
<tr>
<td>23</td>
<td>Design, Mechanical, Electrical, Civil, Chemical and Nuclear Engineers</td>
</tr>
<tr>
<td>24</td>
<td>Safety / Licensing Engineers, including safety and security</td>
</tr>
<tr>
<td>25</td>
<td>Safety/Security</td>
</tr>
<tr>
<td>26</td>
<td>Analysts</td>
</tr>
<tr>
<td>27</td>
<td>Vendors</td>
</tr>
<tr>
<td>28</td>
<td>State Safety Inspectors</td>
</tr>
<tr>
<td>29</td>
<td>State Security Inspectors</td>
</tr>
<tr>
<td>30</td>
<td>IAEA Inspectors</td>
</tr>
</tbody>
</table>

Insider Groups

<table>
<thead>
<tr>
<th></th>
<th>Insider Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Managers</td>
</tr>
<tr>
<td>2</td>
<td>Operators</td>
</tr>
<tr>
<td>3</td>
<td>Technicians</td>
</tr>
<tr>
<td>4</td>
<td>Guards</td>
</tr>
<tr>
<td>5</td>
<td>Visitors</td>
</tr>
</tbody>
</table>

Figure 24-5. Potential Insider Groups

List Attributes

For each of the defined insider groups, characterize their attributes. List the keys that they have, the special privileges that they have, the special knowledge that they have, and the target areas where they have routine access. Continue to list every attribute that might have a bearing on the effectiveness of the security system to counter them as an adversary. Figure 24-6 lists some attributes to consider during the grouping process.
### Evaluating the Physical Protection System Design

#### 24.5.4 Use System Approach for Prevention and Protection

**Analysis Process**

The effectiveness of preventive measures is difficult, if not impossible, to quantify. However, these measures are reasonable and prudent precautions even if their effects cannot be quantified. As a first step, a systematic review should be performed to indicate which preventive measures are in place and properly applied.

The emphasis in the analysis process is on assessing the effectiveness of the protective measures to counter a malicious act. The approach involves developing credible insider scenarios, including collusion scenarios and protracted theft scenarios as appropriate, and then evaluating the protection system effectiveness against them.

The development of credible scenarios consists of identifying the combination of events necessary to accomplish the malicious act. For sabotage, we are concerned with the actions that must be accomplished to initiate a sequence leading to unacceptable radiological consequences. Sabotage scenarios should include both single and multiple target attacks. For unauthorized removal of nuclear material, actions that must be successfully accomplished to remove nuclear material from the facility should be identified. Unauthorized removal scenarios should include situations in which the insider leaves the facility directly with the stolen nuclear material or hides this material on site, taking it out later under more favorable circumstances. Both protracted and abrupt theft should be considered.

**Action Sequences**

Around each target there are a series of protection layers. In most cases, these are the same layers identified in the development of an adversary sequence diagram during the outsider analysis process. Within each protection layer, there are path elements that the insider might use to move from one area to another.
another. Each path element should have some protection measures to defend against the insider. The development of an insider action sequence is similar to the development of an outsider path. The difference, however, lies in the fact that an insider may attack more than one target to accomplish his goal, and he may bypass many, if not all, of the protection measures. An example will be used here to illustrate the process. The target will be reactor sabotage from the control room. The general action sequence is

1. Enter the protected area
2. Enter the control room
3. Sabotage the reactor from the control room
   3.1 Trip circuits
   3.2 Disable pumps
   3.3 Open coolant valves

For the first two steps in the sequence, the insider has some path options. To minimize detection in Step 3, the insider has “action” options, such as covertly disabling alarms or defeating closed-circuit television (CCTV) and personnel surveillance, rather than path options. Figure 24-7 illustrates this case.

![Figure 24-7. Action Sequence Options](image_url)

Protection Measures

The measures used to detect, delay, and respond to malicious acts can be identified and quantitatively analyzed. Likelihood of detection, access delay times, and the timeliness of response are often quantifiable and thus provide a basis for effectiveness analysis. These measures should be identified on the action sequence diagram and listed in a table for evaluation against insider defeat strategies.

Defeat Strategies and Protection Measure Effectiveness

Defeat strategies are developed by considering insider access, authority, and knowledge to overcome the detection, delay, and response features. By examining path elements characteristics, insider attributes, and potential insider defeat strategies for a required sequence of insider actions, credible
insider defeat strategy options can be developed. It should be noted that paths for bringing contraband material into a facility or for unauthorized removal of nuclear material from a facility may not be the same as the path used by the insider himself.

The effectiveness of the specific protection element features against the different potential insider defeat strategies should be assessed quantitatively, as illustrated in Figure 24-8, for each insider group.

<table>
<thead>
<tr>
<th>Insider Action</th>
<th>Protection Measure</th>
<th>Insider Strategy</th>
<th>$P_D$</th>
<th>Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 1</td>
<td>Portal</td>
<td>Normal Entry</td>
<td>0.0</td>
<td>120 sec</td>
</tr>
<tr>
<td></td>
<td>Perimeter</td>
<td>Breach</td>
<td>0.5</td>
<td>300 sec</td>
</tr>
<tr>
<td>Layer 2</td>
<td>Door</td>
<td>Normal Entry</td>
<td>0.0</td>
<td>60 sec</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Breach</td>
<td>0.9</td>
<td>300 sec</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deceit access</td>
<td>0.7</td>
<td>180 sec</td>
</tr>
<tr>
<td>Layer 3</td>
<td>Alarms</td>
<td>Disable</td>
<td>0.7</td>
<td>2700 sec</td>
</tr>
<tr>
<td></td>
<td>CCTV/Operations</td>
<td>Disable/kill</td>
<td>0.1</td>
<td>225 sec</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Act surprised</td>
<td>0.9</td>
<td>105 sec</td>
</tr>
</tbody>
</table>

Figure 24-8. Defeat Strategies and Protection Measure Effectiveness – “Operator” Insider Attempting Control Room Sabotage

The development of credible scenarios consists of identifying the combination of defeat strategies and protection measures with the highest probability of success for the insider to accomplish the malicious act. This is accomplished by superimposing the information from the defeat strategy/protection measures effectiveness table to the action sequence diagram, and then selecting the most advantageous action sequence for the insider. The paths, the sequence of actions along the path, the protective measures encountered, and the optimum defeat strategies are now all taken into consideration. An example is shown in Figure 24-9. Detection probabilities for the optimum defeat strategy for a specific insider are listed in blue at the lower left of the path element or insider action. Delay values are listed in red at the lower right of each element. These values are derived from appropriate strategy and effectiveness tables for specific insider groups.

In some cases, the required actions for completion of the malicious act can be performed over an extended period, and may not follow a specific sequence, so the concept of a continuous path may not always be relevant.

For comprehensive insider analyses, pairing all identified targets and all
24. Insider Analysis

defined insider groups should be considered.

The final step in the analysis is to make a judgment on the effectiveness of the response forces to neutralize a detected adversary. In a theft scenario, the adversary is moving outwards and the security response force is generally moving inwards. Since the response force knows where to go and what to do to contain the adversary, the probability is high that the response force will be able to neutralize the insider. Often the effectiveness of the response force is determined to be 1.00 and therefore the $P_D$ obtained from this analysis is the system effectiveness.

For the case of sabotage, the security response force may not be able to reach a denial position or even to interrupt the insider before completion of the sabotage act. In this event, safety operations may be initiated to mitigate the consequences of the sabotage. This should always be included in the insider analysis.

24.5.5 Evaluate and Summarize Results

Once detailed insider scenarios have been developed, the effectiveness evaluation is completed by considering the accumulated detection, assessment, and delay, and by overlaying the response and mitigation on the insider scenarios. The response effectiveness considers both the effectiveness of interrupting and neutralizing the insider, and the effectiveness of preventing or mitigating the consequences. Insider efforts to reduce response effectiveness should be considered.

The evaluation process should be repeated for every credible scenario for all insider groups and target combinations. The protective measures effectiveness should consider the results of all the evaluations above. An example table showing summarized results for five defined insider groups
attempting control room sabotage is shown in Figure 24-10.

![Figure 24-10. System Effectiveness against Control Room Sabotage](image)

### 24.6 Summary

**Use a Variety of Measures to Counter the Insider Threat**

The insider is considered to be one of the greatest threats that a security system will encounter because the insider has the unique attributes of access, authority, and special knowledge. Therefore, it is imperative that effective measures be taken to prevent insider incidents. A combination of preventive and protective measures offers the best solution to mitigating the insider threat. These include an employee screening process, security awareness education, physical protection systems, and policies and procedures ensuring appropriate handling and controls of attractive target materials.