SAND2014-0937P

Nuclear Security Culture

Workshop Overview

Partnership for Nuclear Security

National Nuclear Security Administration

Workshop Overview

- Evolution and Importance of Nuclear Security Culture
- Overview
- Reflections on Nuclear Security Culture
- International Nuclear Security Resources
- Nuclear Security Culture from Different Perspectives Throughout an Employee's Career
- Training Videos/Case Studies

Presentation

- Discussion questions used throughout
- Case studies and discussion questions to illustrate concepts

Participant Introductions

- Name
- Organization
- What do you think Nuclear Security Culture is?
- Expectations for Workshop

Logistics

- Emergency exits
- Schedule
- Breaks
- Facilities

Summary

By the end of this workshop, you should:

- Have been exposed to Nuclear Security Culture from different country perspectives
- Be able to describe IAEA's concept of Nuclear Security Culture
- Be able to identify implementation options for enhancing Nuclear Security Culture

Nuclear Security Culture

Discussion on Culture

Partnership for Nuclear Security

National Nuclear Security Administration

Culture – One Definition

The assembly of

- Characteristics
- Beliefs
- Attitudes

that reflect a society's capacity for learning and transmitting knowledge to succeeding generations

How would you describe the the your Culture?

Small Group Discussion
15 minutes

Within your culture, how are the following considered?

- Manager privileges
- Unsafe working conditions
- Following the rules
- Reporting problems to managers
- Keeping documentation current

How many of you believe that the threat to nuclear materials and nuclear facilities is real?

Why or why not?

Nuclear Security Culture

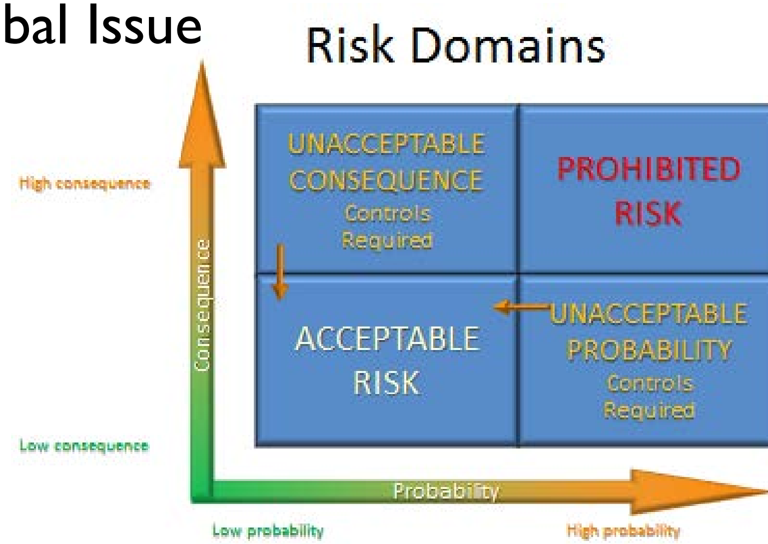
Fundamental Principle F

All organizations involved in implementing physical protection should give due priority to the security culture, to its development and maintenance necessary to ensure its effective implementation in the entire organization.

- INFCIRC/225/Revision 5 and the Amendment to CPPNM

Importance of the Topic

- Threats to Nuclear Security are real
  - Nuclear weapons
  - Nuclear material used in an improvised nuclear device
  - Radioactive material for radiological dispersal device
- Nuclear Security is not only focused on material, institutional knowledge can also be exploited
- Nuclear Security is a Global Issue



Nuclear Safety Culture

"That assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance".

Based upon:

- Openness
- Transparency
- Information Sharing

Ensure that human actions are consistent, appropriate, and correct and human error is minimized or prevented.

Nuclear Security Culture

Security Culture

"The assembly of characteristics, attitudes, and behaviour of individuals, organizations, and institutions which serves as a means to support and enhance nuclear security."

Based upon:

- Compartmentalization
- Secrecy/Confidentiality
- Classification

Relies heavily on the trustworthiness, honesty, and integrity of individuals not to perform malicious acts.

Synergy Between Safety and Security

- Shared principal objective of "*the protection of people, society, and the environment from the effects of harmful nuclear radiation*"
- Shared Attributes:
  - Recognized values
  - Leadership needed for success
  - Accountability
  - Personal dedication and accountability
  - Questioning attitudes, but rigorous approaches to actions
  - Learning and experience driven
  - Best when fully integrated into the system

Both require a coordinated response

Security	Safety
• Considers deliberate acts • Emphasizes confidentiality management • Involves organizations not related to nuclear	• Considers unintentional acts • Emphasizes open information management • Involves only organizations related to nuclear

Sometime the two can conflict such as in emergency egress

Some Differences

- What are some of the visible indicators of a nuclear safety culture?
- What are some of the visible indicators of a nuclear security culture?

Indicators of a Weak Nuclear Security Culture

- Lack of threat awareness
- Lack of security visibility
  - Different security environment for different people at the same position
  - Security exceptions for managers
  - Disregard for security rules/personnel
- Ambiguous security roles and responsibilities
- Poor operational security: "loose lips sink ships"

More Signs of a Weak Culture

- Lack of quality assurance program
  - Substitution of inferior equipment
  - Unskilled personnel
  - Deficiencies in acceptance testing
- Poor record keeping
  - Material inventories, configuration management
- No security training, exercises
- Poor information/cyber security
- Cultural biases
  - Ethnic, tradition

Signs of Strong Nuclear Security Culture

- Defined security policies and procedures that are well documented, understood, and trained to
- All levels of management and management follow the procedures
- Understanding the threat is real and changes in security procedures may be necessary
- Management participation in changes with a positive attitude communicated to staff
- Mechanism for addressing security concerns

Summary

- National culture can impact nuclear security culture
- There is synergy between nuclear safety culture and nuclear security culture
- There are visible indicators of both weak and strong security cultures and an organization may exhibit both

Nuclear Security Culture

Nuclear Security Model

PNS
Partnership for Nuclear Security

NNSA
National Nuclear Security Administration

International Resources

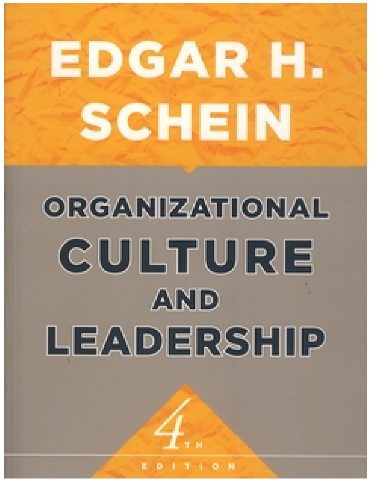
- International Atomic Energy Agency
  - Nuclear Security Series Implementing Guide on Nuclear Security Culture, NSS-7
  - Nuclear Security Series Implementing Guide on Preventive and Protective Measures Against the Insider, NSS-8
  - Coordinated Research Project on Nuclear Security Culture Self Assessment
  - IAEA Course on Nuclear Security Culture

Other International Resources

- World Institute for Nuclear Security
  - Nuclear Security Culture
  - Managing Internal Threats
  - Human Reliability as a Factor in Nuclear Security
  - An Integrated Approach to Nuclear Safety and Security

Organizational Culture and Leadership

- Edgar Schien Model of "Organizational Culture and Leadership" (1997)
- Notice this is an "Organizational" Model
- Layers range from invisible and non-measurable to visible and measurable
  - Visible layers have Performance "Characteristics" which can be identified from "Indicators" (These terms are important in this workshop)
  - Must infer what is invisible from the visible
- Bottom layer (invisible) is the base for the more visible characteristics
  - Credible threat exists
  - Nuclear security is important

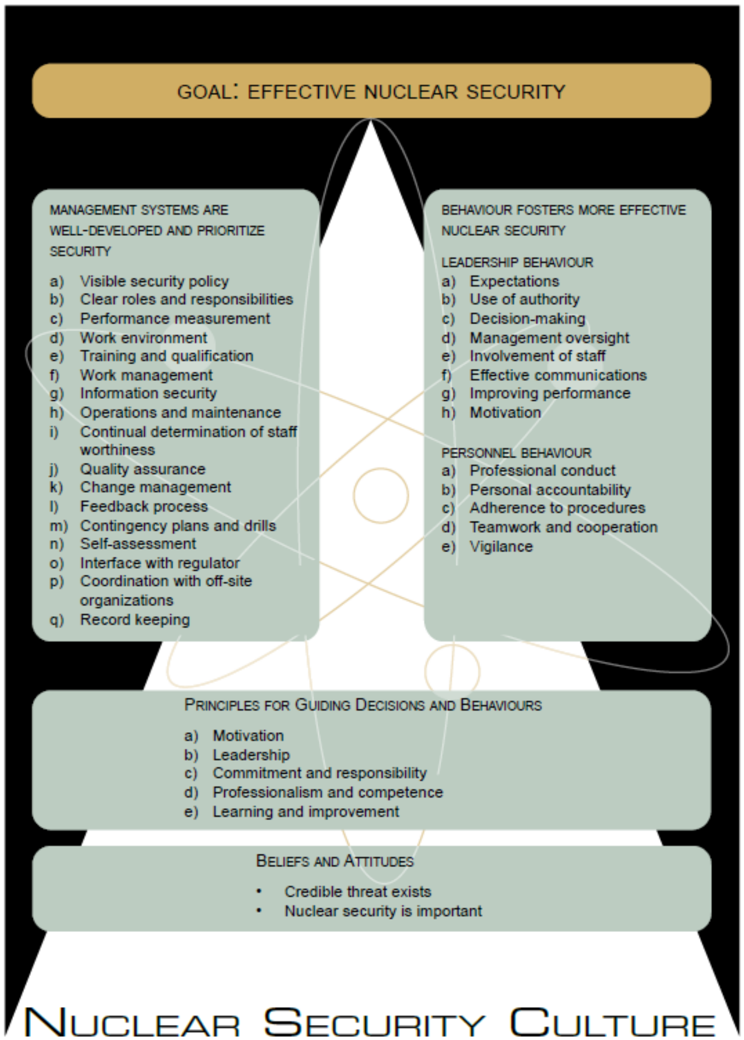


Nuclear Security Culture Beliefs and Attitudes

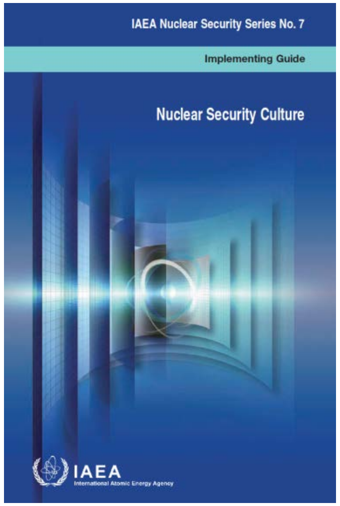
- Credible threats exist
- Nuclear Security is important

Everyone has a role.

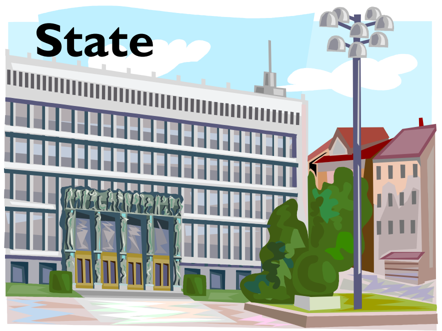
IAEA Model for Nuclear Security Culture



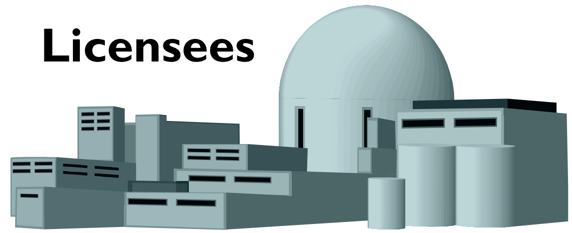
IAEA Nuclear Security Series NSS-07



Nuclear Security Roles



Licensees



Managers

Nuclear Security Culture

IAEA

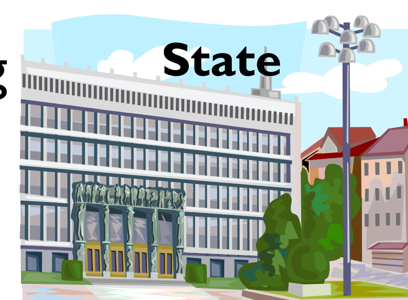
International Community

Public

Employees

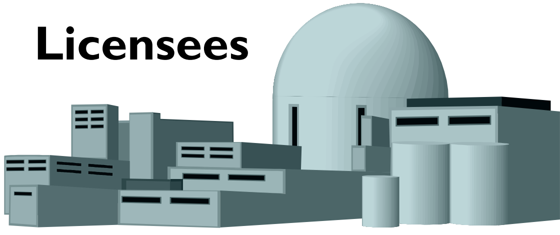
State

- Responsible for establishing a legislative and regulatory framework that fosters an effective nuclear security culture
  - Security policy
  - Protection of sensitive information and of facilities
  - Establishing a legal framework
  - Distribution and coordination of responsibilities especially for associated competent authorities
  - Coordination mechanisms for
    - Exchange of knowledge and data
    - Joint exercises for contingency planning response



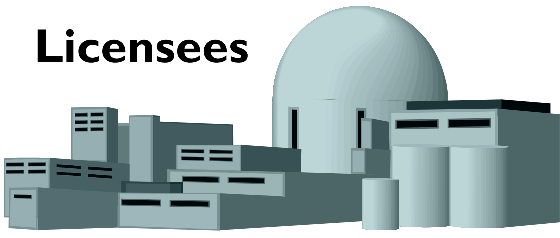
Licencees

- Nuclear security policy consistent with that of the State
- Clearly defined roles, responsibilities, and accountability for each level of the organization
  - Appointed individual with sufficient authority, autonomy, and resources to implement and oversee nuclear security activities
  - Procedures to facilitate rapid resolution of questions
- Resources – financial, technical, human



Licencees

- Management systems to
  - Define expectations
  - Implement and maintain processes
  - Measure progress
  - Assess compliance
  - Improve performance including review and improvement processes
  - Manage change



Managers in Organizations

- Responsible for ensuring appropriate standards of behavior and performance associated with security
- Establish formal decision-making mechanisms
- Maintain effective communications
- Provide training and professional development
- Ensure that staff members are appropriately motivated and that their role in enhancing nuclear security is recognized and valued
- Prevent complacency from compromising overall security objectives

Managers

Employees/Personnel

- Accountable for their own behaviors
- Motivated to ensure nuclear security
- Conduct themselves in a manner that recognizes the circumstances and potential consequences of their behavior
- Comply with facility procedures
- Avoid divulging any information that could undermine security
- Understand how their particular role and interfaces contribute to maintaining security

Employees

Public

- Awareness that security is a key consideration for plant operation
- Understanding that details related to security cannot be divulged
- View nuclear security culture as a sign of professionalism, skill, and responsibility by all actors involved in the protection of nuclear materials and nuclear facilities

Public

International Community

- Provide guidance and support for developing regulatory and institutional infrastructure
- Assist States in meeting obligations and commitments

IAEA

International Community

Foundations of Nuclear Security Culture

- Belief by all that the threat is real
  - Threats exist
  - And can happen at any time

- Supported by all levels of an organization
  - Senior management
  - Managers
  - Staff

Principles

- Motivation
- Leadership
- Commitment and responsibility
- Learning and improvement
- Professionalism and competence

Management Systems

- Visible security policy
- Clear roles and responsibilities
- Performance measurement
- Work environment
- Training and qualification
- Work management
- Information security
- Operations and maintenance
- Determination of staff trustworthiness
- Quality assurance
- Change management
- Feedback process, contingency plans, and drills
- Self-assessment
- Interface with the regulator
- Coordination with off-site organizations

Behavior

- Observable action or statement
- Includes vigilance, questioning, executing work accurately, and adhering to high standards

Leadership

- Expectations
- Use of authority
- Decision-making
- Management oversight
- Involvement of staff
- Effective communications
- Improving performance
- Motivation

Personnel

- Professional conduct
- Personal accountability
- Adherence to procedures
- Teamwork and cooperation
- Vigilance

Summary

- Nuclear Security Culture is based upon the belief that the threat is real and that everyone has a role in security
- Nuclear Security Culture and Nuclear Safety Culture share principal objectives and many attributes

Nuclear Security Culture

Self-Assessments

Partnership for Nuclear Security

National Nuclear Security Administration

Role of Self-Assessments

1. Provides a basis to establish a baseline
   a) Survey
   b) Observation/Interviews
2. Allows analysis of findings to identify actions
   a) Policies and Procedures
   b) Programs and Training
3. Provides a mechanism to communicate
   a) What the changes are
   b) Why they are being made

Individual Exercise

- Complete the sample self assessment individually
- When you have completed the self assessment, rank your organization according to the scale on the back
- You have 30 minutes

Organizational Security Culture

Level	Count
1	
2	
3	
4	
5	

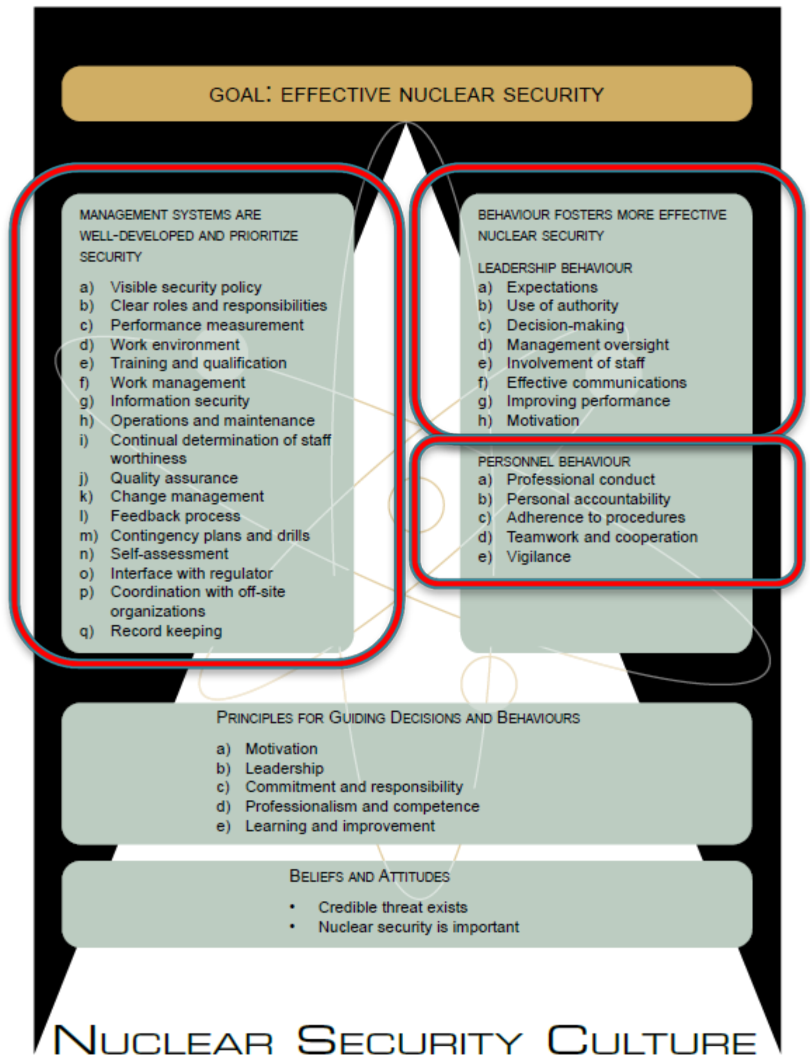
What constitutes the range of levels?

Survey Questions

- The exercise included a small sample
- There is a handout that includes other questions that could be used covering all areas of nuclear security culture
- The IAEA will be publishing a self-assessment guide that can be used to develop such surveys

Security Culture Indicators for Self Assessment

- Management Systems
- Leadership Behavior
- Personnel Behavior



Self Assessment Methods

- Surveys
- Interviews
- Document Reviews
- Observations
- Trends Analysis

1. Pick an area of concern
2. Select the best method for collecting data
3. Collect data
4. Analyze results
5. Decide on changes

Don't do it all at once!
Let culture evolve!

Interpreting Results

- For each area of nuclear security culture
  - Decide how it should look if properly implemented
  - Does current practice match?
  - What is the best approach for achieving desired results?
- Communicating results and how changes will be implemented

Summary

- There are international resources to help with Nuclear Security Culture
- There is value in using a self-assessment to:
  - Establish a baseline
  - Analyse results for improvements
  - Communicate changes and why

Exercise 2
Nuclear Security Culture
Sample Self Assessment

1. Do I think an attack at my facility could really happen?	☐ Yes ☐ No
2. Do I understand my security responsibilities?	☐ Yes ☐ No
3. Does my management act as positive role models for nuclear security culture by setting a good example?	☐ Yes ☐ No
4. Do I believe I have a personal influence on the behavior and attitude of my peers?	☐ Yes ☐ No
5. Would I take action to report a suspicious action or a security concern about a fellow employee or contractor?	☐ Yes ☐ No
6. Do I know what to do if something goes wrong with security?	☐ Yes ☐ No
7. Do I understand what the security procedures are and the reasons for them?	☐ Yes ☐ No
8. Am I regularly informed on security matters affecting the facility?	☐ Yes ☐ No
9. Are there improvements I could make to existing security procedures?	☐ Yes ☐ No
10. Am I taking any security shortcuts?	☐ Yes ☐ No
11. Do I know how to report security problem I observe?	☐ Yes ☐ No
12. Does facility management encourage and support staff to report security problems?	☐ Yes ☐ No

1. Do you think the security measures at your facility are:
   ☐Too Little ☐Too Much ☐ Just Right

2. Based on these answers, do you think you have a weak or strong nuclear security culture within your organization?

3. Based on the WINS Levels of Organization Security Culture, how would you rate nuclear security culture within your organization?

4. Where do you think improvements could be made to enhance nuclear security culture within your organization?

WINS Levels of Organizational Security Culture

Level	Characteristics
1	1. Security is defined and thought about only in terms of compliance with regulations at minimum cost. 2. Security is not seen as a key business risk, and the postulated threats are not considered to be real. 3. Security is seen as the sole responsibility of the Security Department and/or Guard Force. 4. Security violations and "short cuts" in procedures are not considered serious. 5. Most frontline staff are uninterested in security and see it as an obstacle to getting their work done.
2	1. Security is seen in terms of regulatory compliance and the adherence to rules and procedures set by the regulator. 2. Security is reluctantly seen as a business risk, but with a sense that it is an "unavoidable financial overhead" and the risk of an incident is extremely small. 3. The Security Department owns the security program and provides only general, periodic reports to Senior Management. 4. Security performance is measured by lagging indicators such as the number of occasions when the regulator has identified security non-compliances. 5. Senior managers are reactive to their involvement in security. Staff comply with security rules, but they consider them to be intrusive.
3	1. Security is recognized as an important business risk and is overseen by an Executive Committee of the Board. 2. The organization is convinced that security threats are real and that staff at all levels should be involved in helping to achieve an effective security culture. 3. The Security Program is understood and endorsed by the organization's senior management. 4. The majority of staff are prepared to support the security objectives, and they take personal responsibility for their own security and those around them. 5. To avoid security lapses, staff are willing to report security concerns when they have reason to question colleagues' actions or motives.
4	1. The majority of staff in the organization believe that security is important from both a moral and economic point of view. 2. Managers and frontline staff understand that security vulnerabilities can be caused by a variety of events and that managerial behaviour needs to constantly reinforce the importance of effective arrangements. 3. Frontline staff accept personal responsibility for security and take appropriate action when security weaknesses are identified. 4. The organization puts significant effort into proactive measures to prevent security weaknesses, including testing the arrangements. 5. Security performance is measured using all data available, including leading indicators.
5	1. The maintenance of an effective, performance-based, performance-tested security program is seen as a core company value. 2. There is no sense of security complacency in any part of the organization. 3. The organization is confident that its security program will protect its employees and assets. 4. All staff give security the same high priority they give nuclear safety. 5. All employees share the belief that security is a critical aspect of their job and that they share responsibility for preventing security incidents.

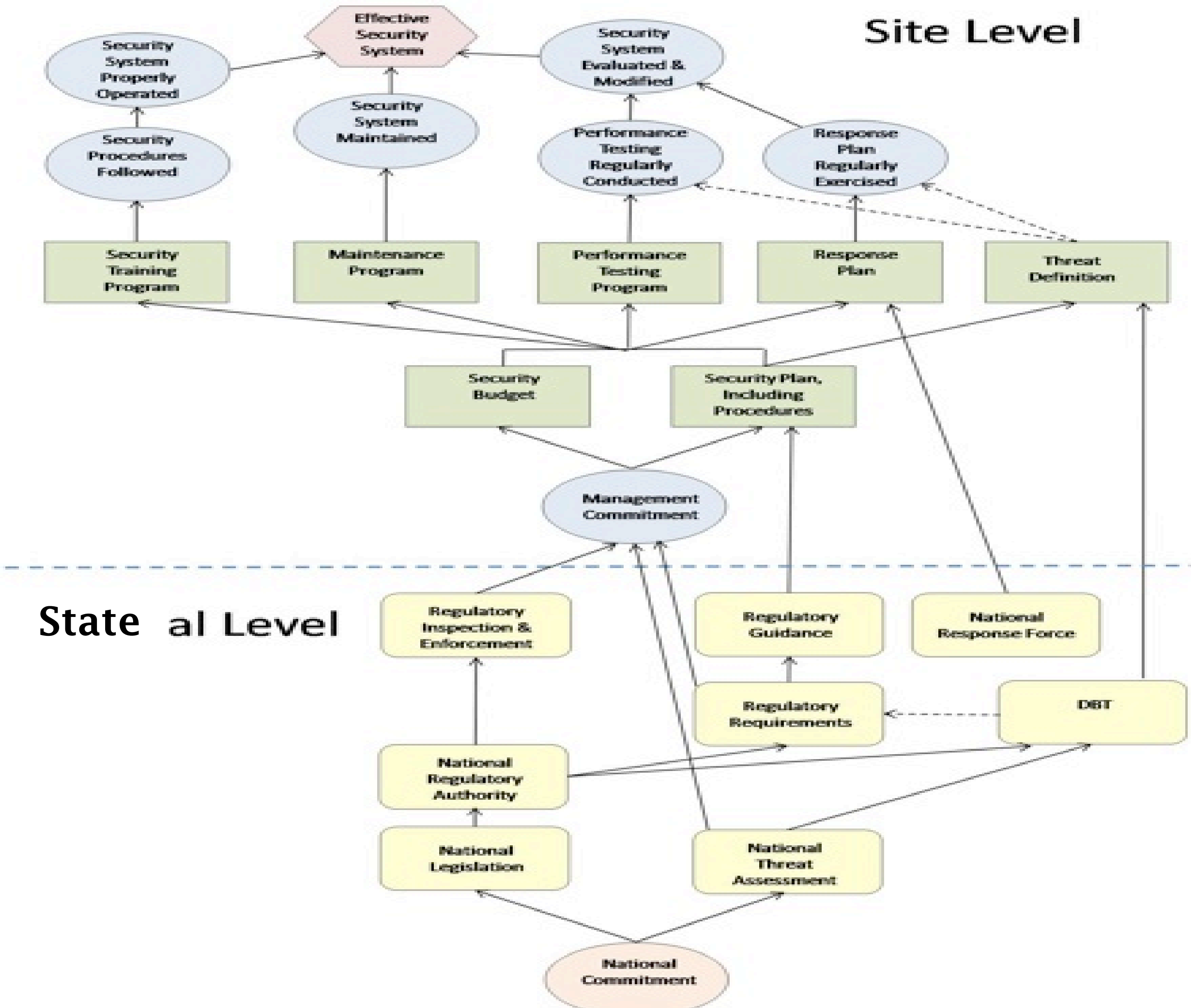
Nuclear Security Culture

Nuclear Security Program Elements and Operational Interfaces

Partnership for Nuclear Security
National Nuclear Security Administration

State Level Organizational Elements

- Legislation
- Regulatory Competent Authority
  - Regulatory Guidance
  - Regulatory Inspection and Enforcement
  - Threat Assessment/DBT
- Response Force Competent Authority/Rules of Engagement
- Nuclear Safety Competent Authority



Site Level
Effective Security System
Security System Properly Operated
Security System Evaluated & Modified
Security Procedures Followed
Security System Maintained
Performance Testing Regularly Conducted
Response Plan Regularly Exercised
Security Training Program
Maintenance Program
Performance Testing Program
Response Plan
Threat Definition
Security Budget
Security Plan, Including Procedures
Management Commitment
State al Level
Regulatory Inspection & Enforcement
Regulatory Guidance
National Response Force
Regulatory Requirements
DBT
National Regulatory Authority
National Legislation
National Threat Assessment
National Commitment

Facility Level Organizational Elements

- Facility Security Organization
- Facility Operational Organizations
- Human Resources
- Facility Security Training Organization
- Financial Management
- Security Engineering and Maintenance
- Performance Testing and Operational Monitoring Organization
- Configuration Management

Facility Security Organization

- An independent organization at the facility capable of:
  - planning
  - resource allocation
  - implementation
  - testing
  - and evaluating

  all aspects of security operations.

- An effective security organization has sufficient authority to carry out all aspects of their duties and is sufficiently independent from other organizations, such as those with production responsibility on site.

Facility Operations

- Facility has administrative systems, physical controls, or written instructions that aid in **minimizing variation** in nuclear and radiological material access, handling, processing, protection and control.
- Facility has written operating procedures/work processes that address threats and vulnerabilities, integrate well with security operations, cover emergency situations on site, and are supported by site management.

Human Resources

- Facilities have a process to appropriately staff program with qualified personnel.
- Security staff has the requisite knowledge, skills, and abilities to perform critical security functions.
- Facilities have capability to assess security staffing needs.
- Facilities have a viable personnel security/trustworthiness program (e.g. HRP, access control, personnel screening)

Facility Security Training Organization

- Facilities can apply local, regional, and national training resources to meet training needs.
- Facilities have the capability to provide on-going site-specific security training and personnel development.
- Facilities have capability to correct operational deficiencies and train staff if needed.

Financial Management

- The site has identified revenue sources for nuclear security program/system support.
- Operational cost data are collected in consistent and useful ways.
- Operational costs are understood and data are used for design decisions and for lifecycle management.
- Nuclear security program can be financially supported by the facility.

Security Engineering and Maintenance

- An organization that assures that security systems at facilities are subject to an ongoing preventative maintenance, calibration, adjustment and cleaning program to assure optimal operation.
- The organization minimizes system downtime and maximize operational life of the security system.
- The organization has sufficient funding, autonomy, and authority for security related tasks.

Performance Testing and Operational Monitoring Organization

An organization that periodically:

- Evaluates the effectiveness of the system, subsystem, and components of the system
- Identifies and corrects deficiencies
- Maintains continuous and effective security operations
- Monitors implementation of security procedures and corrects operational deficiencies

And has sufficient autonomy, authority, and funding.

Configuration Management

- The organization is responsible for assuring that changes are not made to a system before a review.
  - Baseline must be established
  - Changes are evaluated to determine impact to security.
  - Likeness is assured between system documentation and field element.
  - Rebaselining occurs as changes are necessary.

Summary

- Each above organizational element is necessary to enable a good nuclear security culture to be implemented and to be sustained.

Nuclear Security Culture

Insider Threat Overview

Partnership for Nuclear Security

National Nuclear Security Administration

Objectives

- To understand (characterize) the insider
- To identify unique insider issues
- To recognize an insider protection approach
- To understand the insider analysis process

Definition

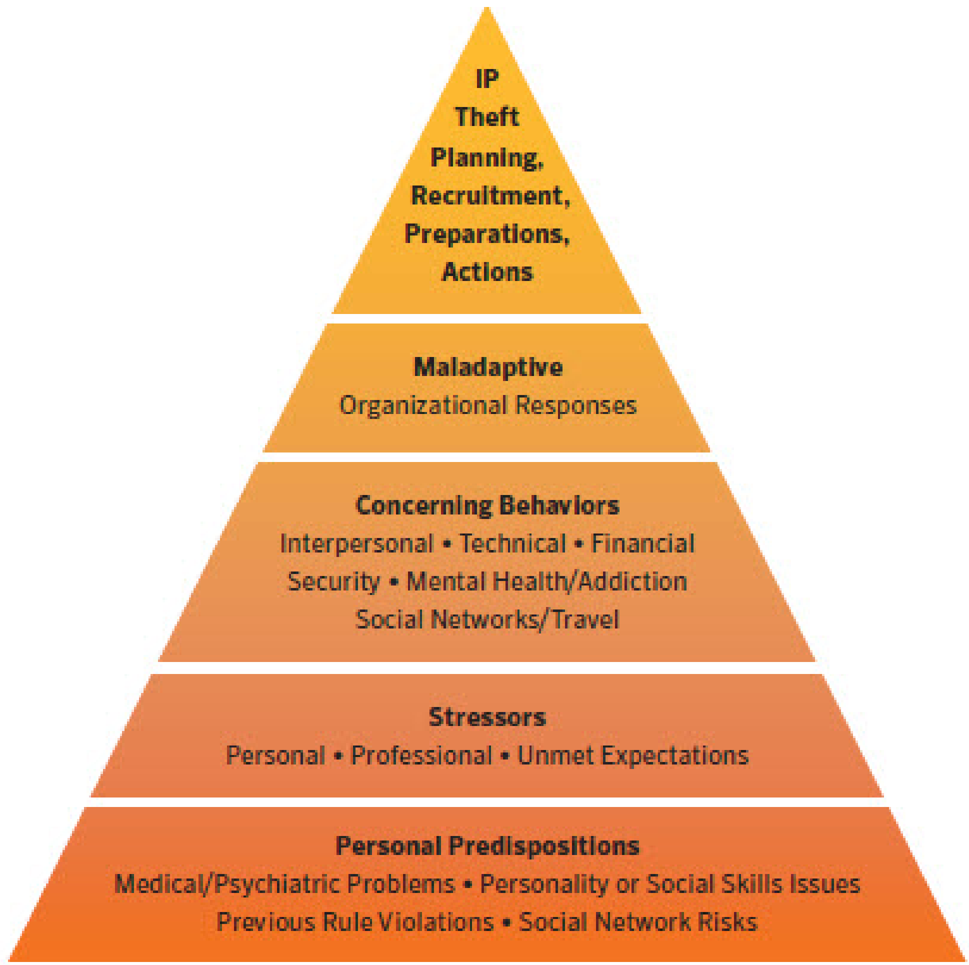
- An insider is any person who has authorized access (either escorted or unescorted) to protected areas, such as
  - Managers
  - Employees
  - Service providers
  - Visitors
  - Inspectors

Potential Insider Motivations

- Ideological—terrorist, environmental, political
- Financial—wants/needs more money
- Revenge—disgruntled employee or customer
- Ego—"See what I am smart enough to do"
- Psychotic—mentally unstable but capable
- Goal directed against government

Motivation may determine the type and extent of malevolence

Critical Pathway Framework



Shaw, Eric, Stock, Harley: "Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading of the Writing on the Wall"

The Creation of the Insider: "The Critical Pathway"

1. Personal predispositions in individuals vulnerable to insider risk present prior to joining the organization
   - A history of serious mental health problems
   - Social skills problems or biases in interpersonal decision-making including a sense of entitlement, lack of empathy for others, insensitivity to the consequences of actions, etc.
   - Previous violations of law, or organizational policies or practices
   - A social or professional network risk such as a friendship, family member, or social or work contact who is affiliated with an adversary or competitor or a source of risk for the employee (an addicted spouse).

Shaw, Eric, Stock, Harley: "Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading of the Writing on the Wall"

The Creation of the Insider: "The Critical Pathway"

2. Examples of personal stressors noted in subjects at-risk for insider acts

- Financial Problems
- Relationship, marital or family difficulties
- Significant medical problems
- Legal problems
- Relocation

Shaw, Eric, Stock, Harley: "Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading of the Writing on the Wall"

The Creation of the Insider: "The Critical Pathway"

3. Examples of professional stressors noted in subjects at-risk for insider acts

- Demotion or failure to achieve anticipated advance
- Loss of seniority or status in merger or acquisition
- Disagreements regarding intellectual property rights
- Transfer
- Disappointing review
- Conflicts with coworkers

Shaw, Eric, Stock, Harley: "Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading of the Writing on the Wall"

The Creation of the Insider: "The Critical Pathway"

4. Examples of concerning behaviors or violations of policy, practices or law observed in subjects at-risk for insider acts

- Disruptive conflicts with coworkers or supervisors
- Violations of information, physical, personnel security
- Violations of financial rules
- Violation of travel policies
- Tardiness or missing work
- Unreported personal or professional social network risks

Shaw, Eric, Stock, Harley: "Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading of the Writing on the Wall"

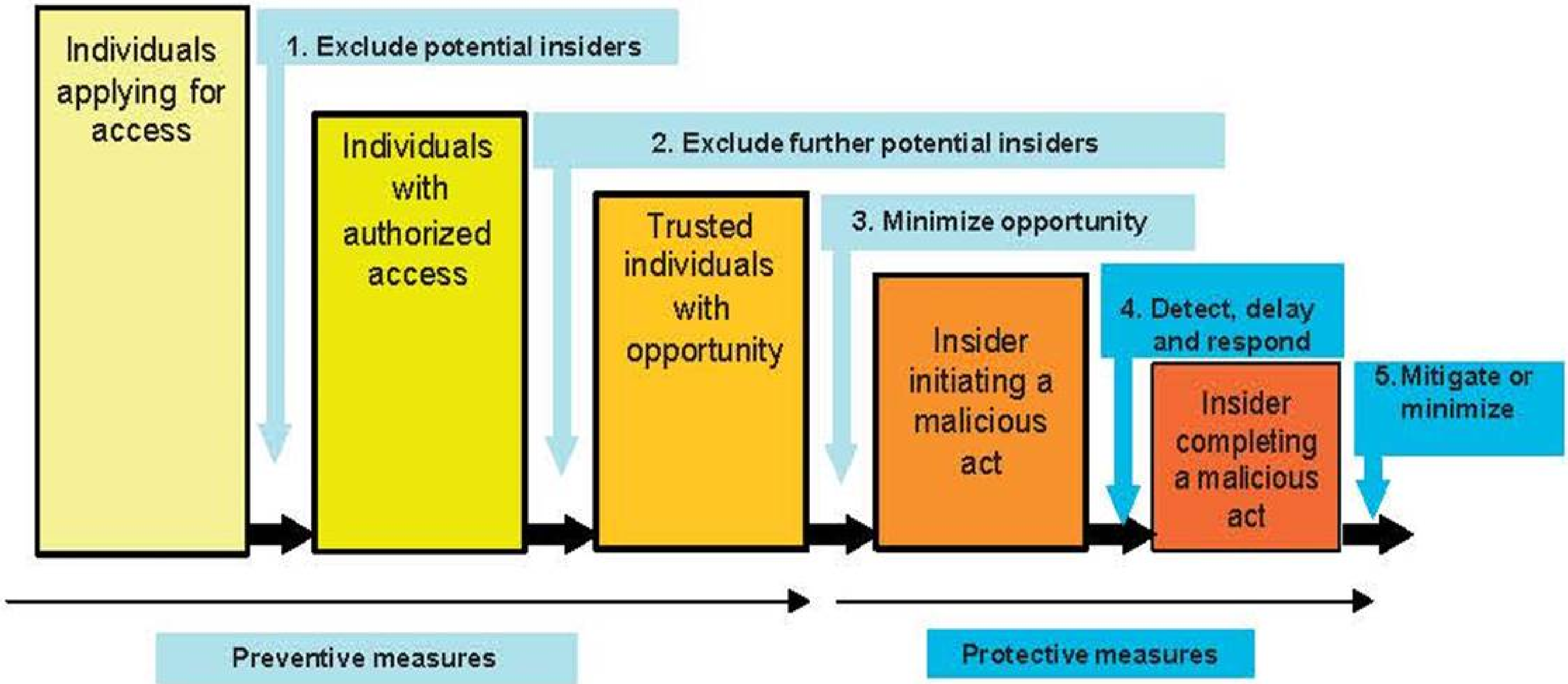
The Creation of the Insider: "The Critical Pathway"

5. Examples of Concerning Behaviors or Violations of Policy, Practices or Law Observed in Subjects At-Risk for Insider Acts

- Disruptive conflicts with coworkers or supervisors
- Violations of information, physical, personnel security
- Violations of financial rules
- Violation of travel policies
- Tardiness or missing work
- Unreported personal or professional social network risks

Shaw, Eric, Stock, Harley: "Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading of the Writing on the Wall"

Measures against Insiders



Insider Summary

- The insider threat presents a unique problem
  - Have a proactive program to identify possible issues
  - Observe on a continuous basis
  - Raise employee awareness

Small Group Exercise: Case Study

Insider

Time: 20 minutes

For the past year, Paul shared an office with Jim. Jim had been with the company for 20 years and always seems over-worked. He never seemed to have time to go out for lunch with the other coworkers or talk about sports in the hallways. The only time that he would take a break from his work was to complain about “stupid company policies” or “incompetent managers”. Although Jim’s rants were annoying at times, Paul didn’t mind sharing an office with him because he mostly kept to himself and focused on his work. Over the course of a few short weeks, Paul began to notice some pretty big differences in Jim’s behavior. Jim not only started going out to lunch, but he offered to pay for everyone. He was always smiling and laughing, things he never seemed to do before. One day after work Paul saw Jim leave work in a very expensive sports car. This didn’t make any sense to Paul because Jim had always complained about not having enough money.

Small Group Discussion:

1. What are the good or bad indicator(s) of nuclear security culture in this case?

2. How would your facility address this scenario?

3. What improvements would enhance nuclear security culture in this case?

Small Group Exercise: Case Study

Insider

Time: 20 minutes

Paul's family routinely asks him for loans that they never pay back. He would feel guilty saying no to them because after all they are family. Until now the requests have been manageable, but Paul's mother has been going through some expensive health procedures. Paul had to put these extra expenses on his credit cards, but he is reaching his credit limit and running out of options. His mother's health is the highest priority so he needs to find another way to find money quickly.

Small Group Discussion:

1. What are the good or bad indicator(s) of nuclear security culture in this case?

2. How would your facility address this scenario?

3. What improvements would enhance nuclear security culture in this case?

Small Group Exercise: Case Study

Insider

Time: 20 minutes

Paul wanted to see if he could do some freelance work on nights and weekends so he posted his resume on a social media site. His resume was very detailed about the type of projects he worked on, how he impacted those projects, and it even stated that he had an active security clearance. Just a few days after posting his resume, he was contacted by someone interested in his work. The contact told him that if he downloaded all of the project files onto a CD he would give him a large amount of money. Although these documents were classified, Paul thought there would be not much harm in sharing the information because the projects had long been finished. Paul went to work the next day and secretly download the files. He sent the CD to the contact and received the large amount of money.

Small Group Discussion:

1. What are the good or bad indicator(s) of nuclear security culture in this case?

2. How would your facility address this scenario?

3. What improvements would enhance nuclear security culture in this case?

Nuclear Security Culture

Recruitment and Hiring

Partnership for Nuclear Security

National Nuclear Security Administration

Phases of Employment

- Hiring
- On the job
- Transfers within the company
- End of employment (usually referred to as "termination")

Recruiting

- Where do you get your employees?
  - Universities
  - Other facilities
  - Other countries
- What educational backgrounds do you recruit?

Recruitment

- Job postings

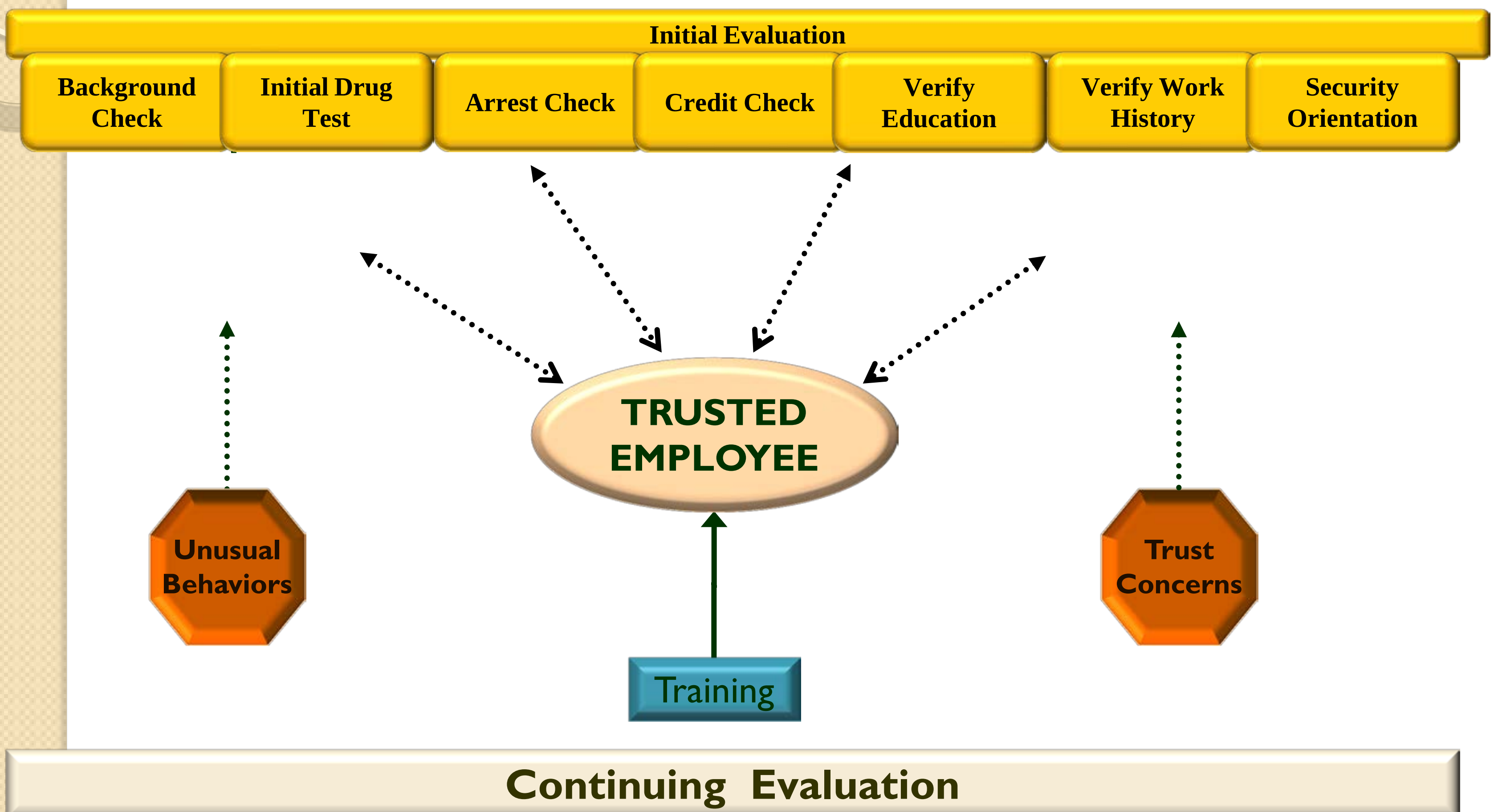
  -Straightforward description of job duties and qualifications
- Testing programs
- Communities of personnel with traits/qualifications
  - Job fairs
  - Academia
  - Related conferences/associations
- Known entities

  -Quality personnel with whom you/trusted coworkers have experience

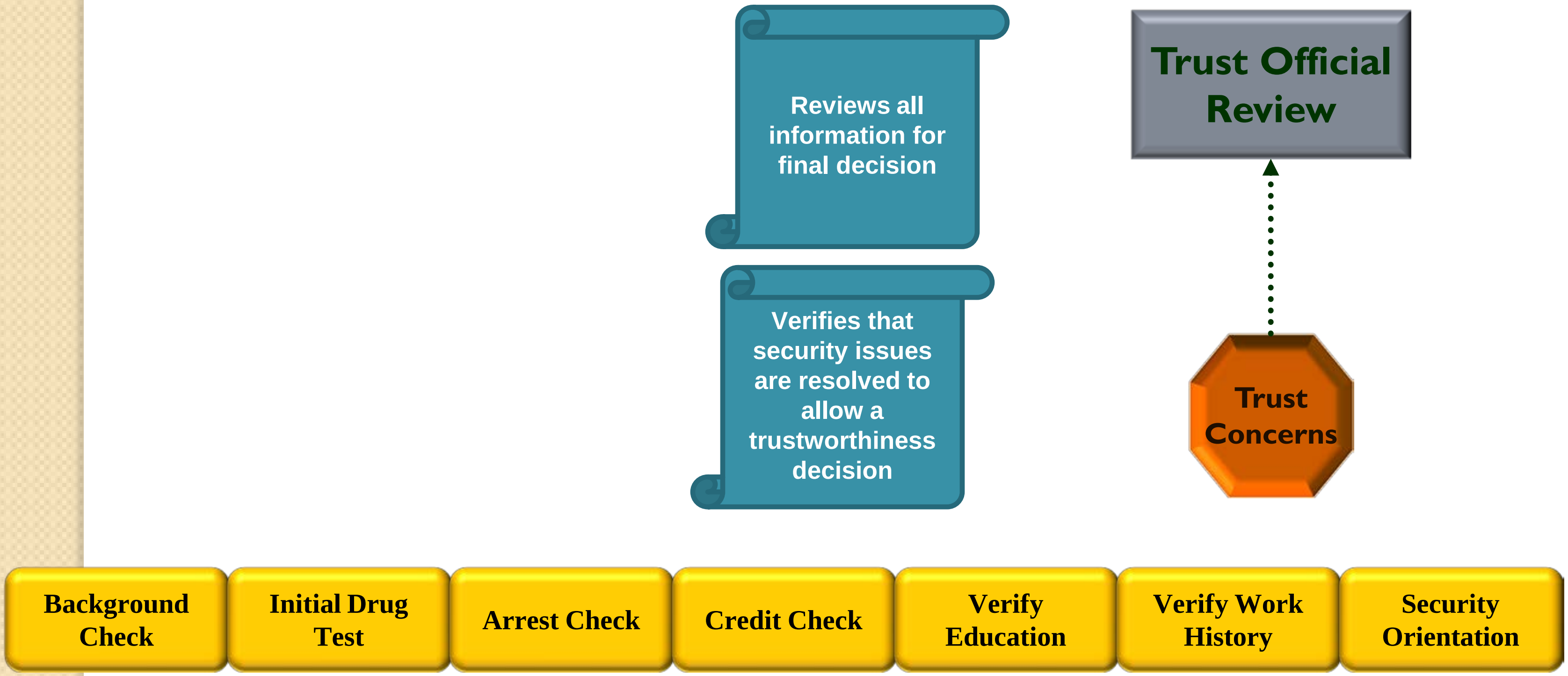
US Personnel Screening

- Interview candidate
- Rapid corporate background check
- Application process
  - Candidate vetting
  - Reference checks
- Extend offer
- Extensive background investigation for clearance
- Periodic reinvestigations

Trustworthiness Program



Trust Official Review



Trust Official has Final Determination

- Based on all the information regarding an individual, the certifying official makes a final decision regarding certification
- A negative decision can be appealed
  - Due process ensures fairness
- The process is repeated every year for recertification

Aspects of Trustworthiness Program

- The process includes:
  - Confidentiality of records
  - Fitness for duty check
  - Awareness of on-the-job security and safety concerns
  - Enhancement of personal safety
  - System of checks and balances ensures fairness to all employees

Program Success

The most important ingredient for success in any trustworthiness program is the honesty and integrity of all involved parties.

Paul Smith

Phone: 555-513-5484
E-mail: paulsmith28@gmail.com

Objectives

Leverage expertise in nuclear design, safety, and project management.

Education

Masters (August 2010)

- Civil Engineering degree from Five Star University
- GPA: 4.0
- President of Engineering Society

Experience

Senior Engineer (December 2010 –September 2013)
ABC Nuclear Company

Incorporated design requirements into analysis and design documents

Provided technical guidance and mentoring to less experienced engineers

Lead engineer on new water pump design

Led the safety team through 5 successful safety audits

Skills

- 6 Sigma Black Belt
- Project Management Professional Certified
- Plant Design
- Mechanical System Design
- Safety initiative lead

Group Exercise: Case Study (20min)

Recruitment and Hiring

Paul is a smart engineer with impressive accomplishments. Managers at Lagassi Nuclear Research Institute were eager to interview Paul after reviewing his resume. Paul skillfully interviewed with several managers and staff. Everyone was enthusiastic with the idea of hiring Paul as soon as possible.

Before an employment offer could be extended, a required, thorough background investigation would need to be completed. The background investigators were diligent, uncovered some interesting facts about Paul.

Background Report – Resume

There a few small lies on Paul's resume:

- His university reported a GPA 3.5, not 4.0. Paul performed poorly on a few non-engineering classes that he did not include in the GPA on his resume.
- As a member of his university's Engineering Society he coordinated several guest speakers, but he was not the President.
- Although Paul took some project management and 6 Sigma classes, he is not a 6 Sigma black belt or a certified project management professional.
- Paul played a small part in the safety team at ABC Nuclear Company, but he was not the lead, nor a major contributor

When asked about these lies during his investigation interview, Paul quickly confessed and was very open and honest about his mistake.

Background Report – Family History

Paul grew up in a very poor family, but through his own hard work was able to do well in school and get a full scholarship to Five Star University. Now that Paul is working, he supports his parents financially. Sometimes his siblings ask for loans that are never repaid. This puts Paul under considerable financial strain.

Paul's older brother, Michael, is currently in prison on gang related charges. Michael will be released from prison in 3 months and will be looking for a job.

During Paul's investigation interview, he confessed that his sister, Rachel, has a skillset in cyber hacking. She has been known to put her skills to use for criminal purposes if the price is right.

Large Group Discussion:

1. Would you hire Paul Smith for an Engineering Support position? Why or Why not?

2. How would your facility address this scenario?

3. Is Paul Smith a potential security risk?

Nuclear Security Culture

Employee Considerations

Partnership for Nuclear Security

National Nuclear Security Administration

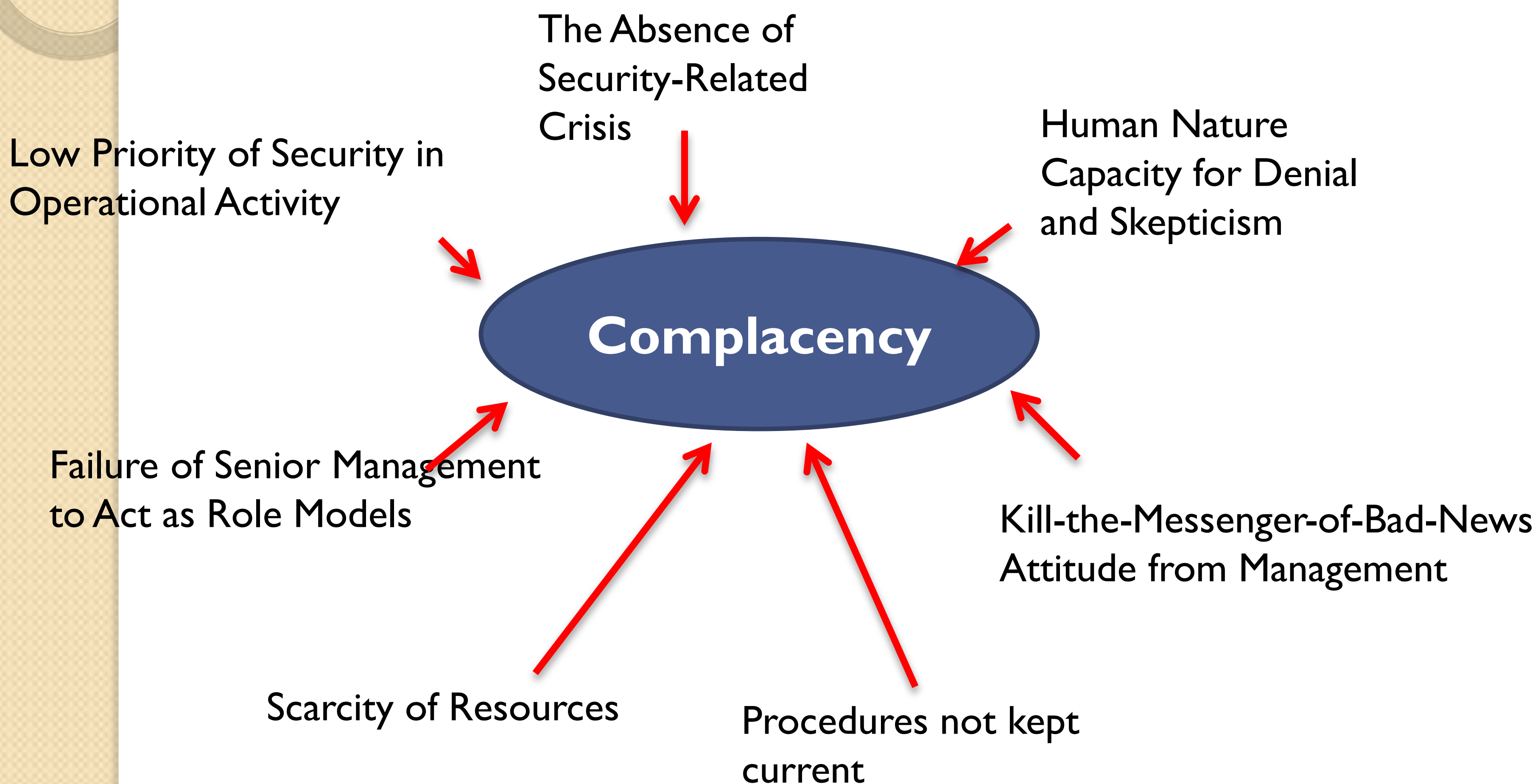
Phases of Employment

- Hiring
- On the job
- Transfers within the company
- End of employment (usually referred to as "termination")

Expected Behavior

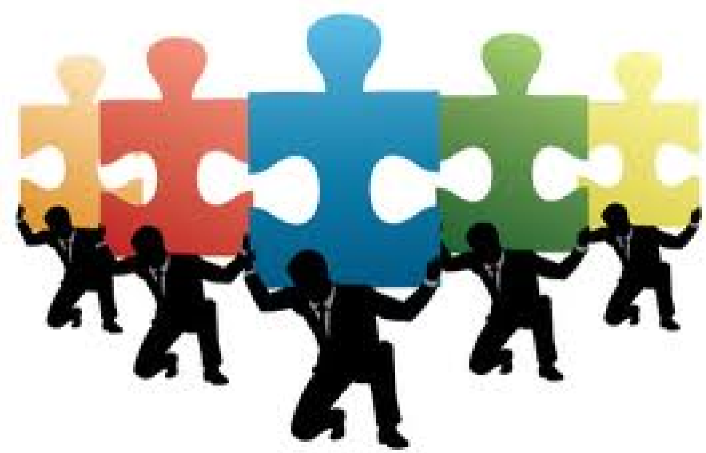
- Professional conduct
- Personal accountability
- Adherence to procedures
- Teamwork and coop
- Vigilance

Biggest Threat to Nuclear Security Culture



Strategies

- Personnel Security Program
  - Employees & Visitors
- Access Control
- Strong Security Training Program
- Employee Concerns Program
- Public Relations



Personnel Security Program

- How is trustworthiness determined?
  - Employees
  - Contractors
  - Visitors
  - Vendors
- How is access authorized?
  - How will access be determined?
  - Escort requirements
  - How will access be implemented for different protection layers?

Access Controls

- Authorized (unescorted access) – who, what, when, where
- Who authorizes access under what criteria
- Procedures for changing authorizations
  - Credentials (badging)
  - Access lists
- Based on need-to-know and least privilege
- Using technology to help enforce two-person rule and duress conditions
- Procedures for exceptions or non-routine access

Other Third-Party Considerations

- Third-parties
  - Regulators/Inspectors
  - Emergency Response Personnel
  - Off-site Response Forces

- Risk assessment
  - Implications of third-party access
    - On-site
    - Remote
  - Application of appropriate security controls

Security Training

- Without good training, security technology cannot be effective
- People provide the strongest assets and weakest links in security
- Strong operational security and nuclear security culture are the strongest defenses against social engineering
- Many security incidents result from human error or complacency
- Security training has many levels and should occur at least annually for all staff

Types and Examples of Security Training

- Awareness
  - Threats and targets
  - Roles and responsibilities
  - Operational security
- Topical
  - Documentation Protection
  - Material handling
- Professional
  - Security managers
  - Guards and response forces
- Specialized
  - Risk management
  - Incident prevention
  - Incident response

Regular Security Training

- Threats to the facility and its assets
- Roles and responsibilities in security
- Information protection
- Security procedures regarding access and escort
- Security procedures during a security event
- Situational awareness and operational security
- How to report events/concerns

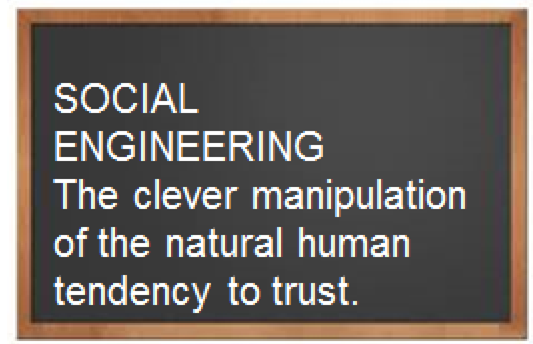
Operational Security

- Being aware of your surroundings during conversations
  - Who might be listening?
  - Could the information being discussed contribute to an attack or unauthorized release of information?

- Being aware of how trash is destroyed
  - How would an adversary view the information?
  - Should the information go into the trash or be shredded?

Social Engineering

- Goal – gain unauthorized access to systems or information
- Method – Exploiting human nature
  - Deceiving
  - Manipulating
  - Bribing
  - Seducing
  - Coercion – blackmailing, threatening family or friends



- Successful because most victims want to trust people and be helpful
- Victims may have no idea they have been tricked into helping or revealing information

Online Social Media

- People share more of their lives than ever on social media
- It is an easy place to
  - Vent frustrations perhaps making a person more vulnerable to coercion
  - Reveal information that when collected with other information reveals something to the adversary

Job Requirements

Understanding of what is required with every change in position, including promotions

- Performance Objectives
- Metrics for Performance
- Security and Safety Responsibilities including:
  - Information confidentiality
  - Two-man rule where applicable
  - Associated security and safety procedures
  - Knowing when job impacts security

Changes in Job

Opportunities

- Training
  - On-the-job
  - Professional development
- Promotions or career changes
- Mentoring
- Succession planning

Security Implications

- Changes in access controls
  - Building or area access
  - Computer accounts
  - Privileges
- Maintenance of need-to know and least privilege principles

Taking Action—Three Choices

- When you see behavior that you think is unusual, you have three options
  - Ignore the behavior
  - Get more information
  - Report the observations immediately
- Remember what is at stake
  - Consider what happens if you fail to report and the worker causes an accident or security infraction
  - You may have to decide which is more important – friendship or safety/security

Employee Concerns Reporting

- Provide mechanism for employees to report security concerns that is
  - Safe from retaliation
  - Supportive in correcting security situations
- Address lessons learned from security incidents without over-reacting
- Ensure that employees are part of the solution

- Provide tracking of incidents

Implementing Nuclear Security Culture Also Includes

- Good public relations with nearby communities relieves negative pressures from community
  - The facility contributes to the common good
  - The public believes you are a secure facility
  - They have a role in maintaining that security

Summary

- Nuclear Security Culture plays a role throughout an employee's career
- Staff need clear, understandable security policies and procedures
- Security education and training is vital
- Strong nuclear security culture is core to personnel security

Small Group Exercise: Case Study #1

During Employment

Time: 20 minutes

Paul is met at the LNRI PTR gate by a coworker who says he has left his badge on his desk. He asks Paul to let him in so he can go get it.

Paul recognizes the coworker as someone he works daily with so lets him in and goes to his own office.

Later, Paul sees the employee with a toolbox in an area he does not normally work in and notices that he is still not wearing his badge. Paul is unsure whether to challenge the coworker or go talk to his manager.

Small Group Discussion:

1. What are the good or bad indicator(s) of nuclear security culture in this case?

2. How would your facility address this scenario?

3. What improvements would enhance nuclear security culture in this case?

Small Group Exercise: Case Study #2

During Employment

Time: 20 minutes

Paul notices an operator in the PTR control room asleep at his desk. He knocks on the control room window and this seems to wake the operator.

When Paul looks again after his experiment, he notices that the operator is again asleep.

He has heard that the operator is a new father and remembers those first days when his children were babies. He decides not to report the operator.

Small Group Discussion:

1. What are the good or bad indicator(s) of nuclear security culture in this case?

2. How would your facility address this scenario?

3. What improvements would enhance nuclear security culture in this case?

Nuclear Security Culture

Human Reliability Program (HRP) – US Example

Partnership for Nuclear Security

National Nuclear Security Administration

What is HRP?

A Human Reliability Program (HRP) is a program designed to ensure that individuals in positions requiring access to certain materials, facilities, and programs meet the highest standards of trustworthiness as well as physical and mental suitability.

Applies to security and safety.

Why HRP?

- The insider is considered by security best practices and the international community to being a significant threat to nuclear security.
- In the nuclear industry, the insider is particularly problematic in that they know the organization and have generally passed security screening process.
- We know from experience that personal problems, such as divorce, substance abuse, death of someone close, or a change in ideology, may have a significant effect on an individual's outlook.

Possible Causes for Security and Safety Concerns

- Physical illness
- Drugs/alcohol
- Psychological disorders
- Stress overload
- Fatigue
- Financial issues

Potential Indicators for Performance Concerns

- Failure to follow standard operating procedures
- Erratic or deteriorating productivity
- Errors in judgment
- Missing deadlines
- Repeated accidents
- Inability to organize a series of activities
- Forgetting to complete a task or part of a task
- Diminishing quality of work
- Inability to concentrate
- Change in work involvement

Taking Action—Three Choices

- Ignore the unusual behavior
- Obtain additional information
- Report your observation

HRP Program Components

- Recognizing the threat
- Defining HRP positions and requirements
- Developing the regulatory base for implementation
- Implementation is an on-going process

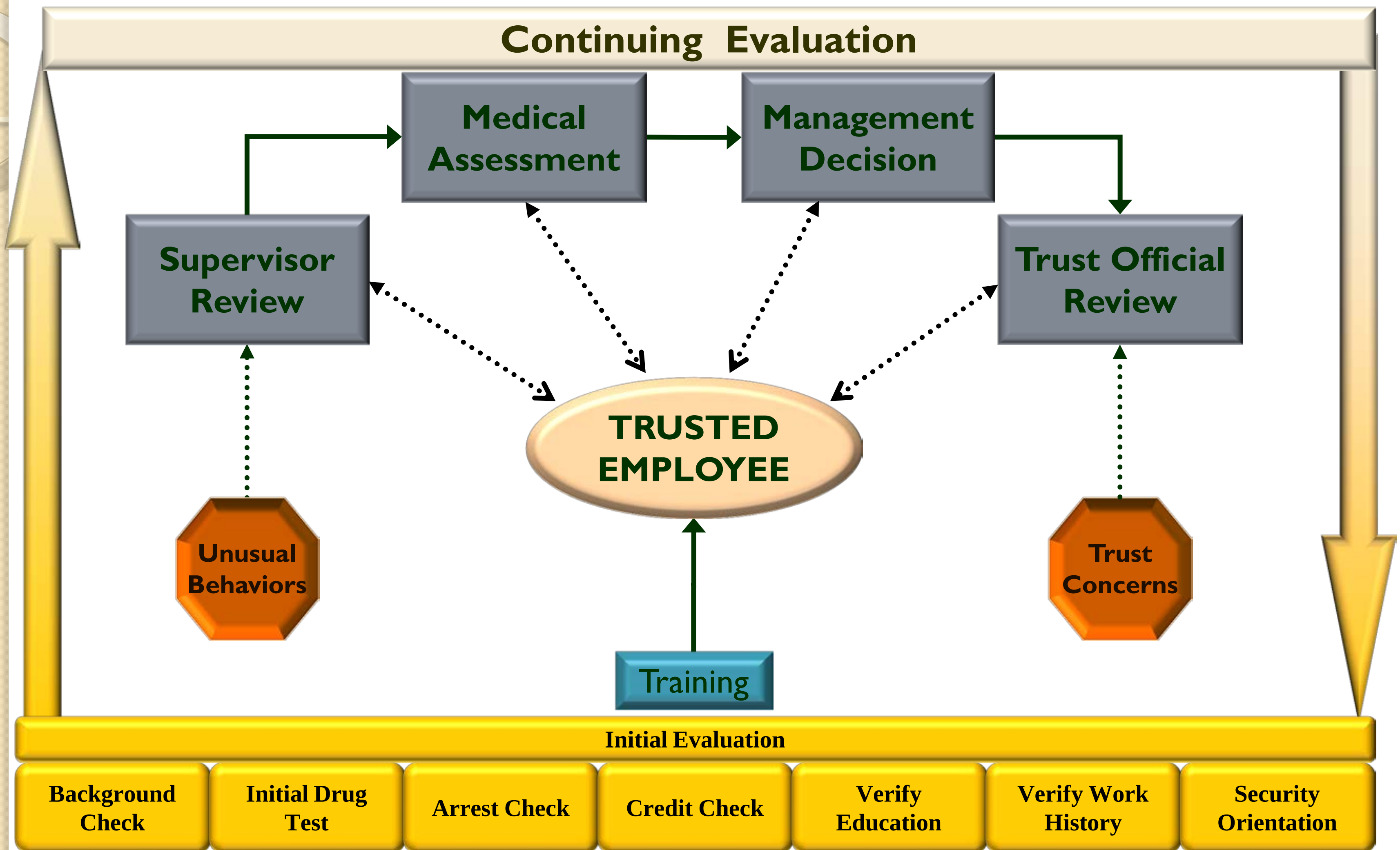
US HRP Process for Individuals in an HRP position

Clearance required for consideration into HRP

The HRP involves four steps

1. Supervisory review – individual/position
2. Medical assessment
3. Management evaluation
4. DOE personnel security review; clearance determination

Each component is completed for initial certification and then every 12 months for recertification


Continuing Evaluation
Medical Assessment
Management Decision
Supervisor Review
Trust Official Review
TRUSTED EMPLOYEE
Unusual Behaviors
Trust Concerns
Training
Initial Evaluation
Background Check
Initial Drug Test
Arrest Check
Credit Check
Verify Education
Verify Work History
Security Orientation

HRP Impacts

- Human interactions invariably rely on the offering of assurance and the receipt of trust. A fundamental element in any human relationship is knowing when to trust and when to doubt.
- HRPs
  - Are not punitive;
  - Are used to assure a person's truthfulness and loyalty to the nuclear security goal;
  - Have a number of elements and may not fit all cultures; and
  - Can vary in scope and have numerous benefits to the workplace.
- The effect of a HRP on potential employees can be immediate and positive:
  - The benefit to overall safety and security is recognized.
  - Knowledge that employment is contingent on an HRP review will ensure high-quality recruits.
  - Conversely, those recruits with malicious intent may also self-select by not applying for employment.

Summary

A structured HRP is a proven systematic approach to mitigating the threats relating to individuals with nuclear and/or radiological materials access and/or knowledge.

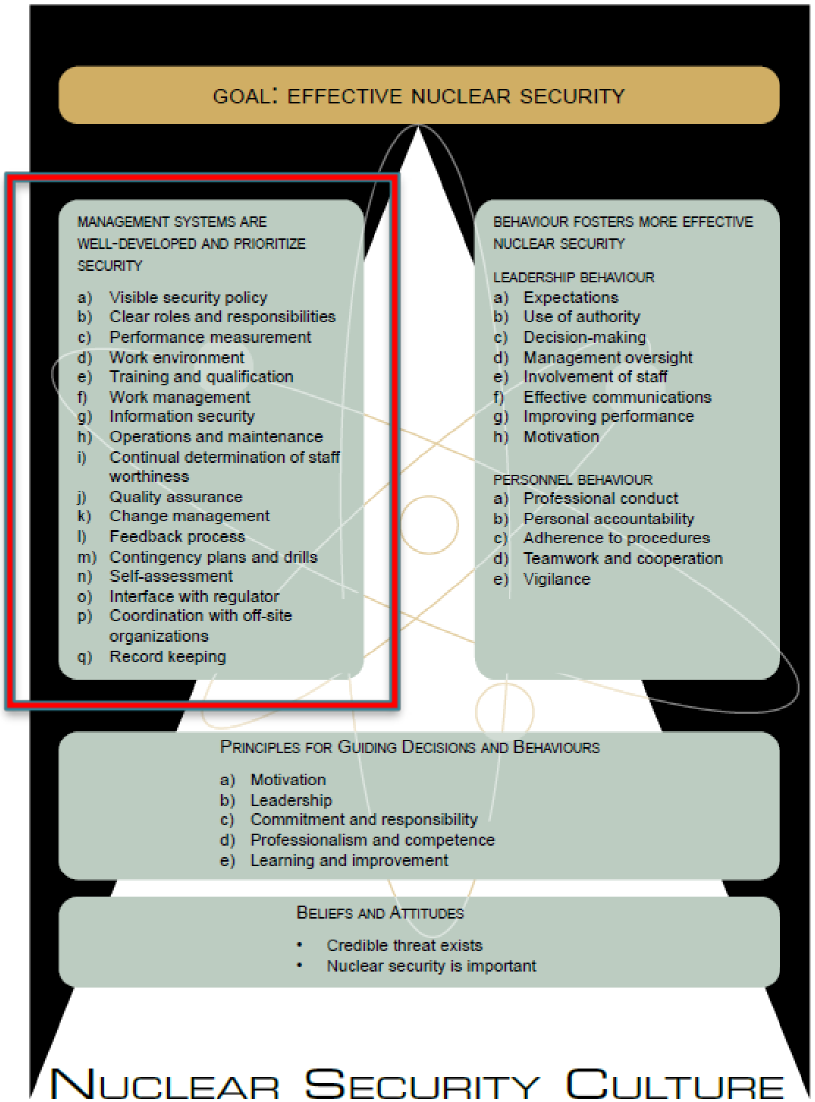
Nuclear Security Culture

Management Responsibilities and Leadership Behaviours

Partnership for Nuclear Security

National Nuclear Security Administration

IAEA Model for Nuclear Security Culture



Management Systems

- Visible security policy
- Clear roles and responsibilities
- Performance measurement
- Work environment
- Training and qualification
- Work management
- Information security
- Operations and maintenance
- Determination of staff trustworthiness
- Quality assurance
- Change management
- Feedback process, contingency plans, and drills
- Self-assessment
- Interface with the regulator
- Coordination with off-site organizations

Management System

- Staff performance affected by management systems:
  - Quality of management
  - Standards for quality of work
  - Training
  - Documented procedures
  - Information systems, etc.
- Well-developed management system is essential feature of effective nuclear security
- Reflects the nuclear security culture

Visible Security Policy

- Should exist and be visible
- Provide a strong statement in support of security
- Relay the highest expectations of management
  - Protection of information
  - Awareness of potential security concerns
  - Vigilance and reporting of all security incidents

✓ Security culture indicators
  - Policy established, posted, and familiar
  - Function respected within organization
  - Code of conduct covers needs of nuclear security
  - On-going training and awareness on code of conduct

Clear Roles and Responsibilities

- Understanding of "who is responsible for what"
- Reviewed and updated periodically
- Timely reflection of organizational changes

✓ Security culture indicators

  - Clearly defined roles and responsibilities for nuclear security positions
  - Staff understands and are encouraged to seek clarification
  - Roles adequately explained to new personnel

Performance Measurement

- Quantified measures of performance associated with identified goals

✓ Security culture indicators

- Benchmarks and targets used to understand, achieve and improve performance
- Results regularly compared to targets
- Action taken when security performance does not fully match goals
- Effective performance leading to better security is rewarded

Work Environment

- Physical and psychological work environment has a large impact on staff performance
- Some impacts are indirect and some direct

✓ Security culture indicators

- Environment conducive to high standards (housekeeping, tools, etc.)
- Staff consulted about ergonomics and effectiveness
- Texts of guides and procedures are clear
- Top managers visit manned security posts

Training and Qualification

- Staff has necessary knowledge and skills
- There is a systematic approach to training and qualification

✓ Security culture indicators

- Training and qualification standards documented, appropriate, and communicated
- Training time has high priority
- Status of staff qualifications is known
- Staff do not perform work for which not qualified
- Physical fitness criteria are established
- Basic security awareness on security and reporting violations

Work Management

- Security work suitably planned to ensure security is not compromised

✓ Security culture indicators
  - Work planning ensures security maintained
  - Contingency plans address possibilities
  - Staff follow established plans or seek appropriate changes
  - Work planned in sufficient detail to ensure effectiveness
  - Interfaces considered when planning work

Information Security

- Controlling access to sensitive information is vital
- Classification and control measures must exist

✓ Security culture indicators
  - Classification and control measures documented
  - Responsibilities assigned for classification and control
  - Clear processes and protocols exist for information security
  - Information is segregated, stored and managed
  - Staff understand importance of controlling information
  - Cyber systems are maintained securely

Operations and Maintenance

- Wide variety of security system are used
  - Accounting and control systems
  - Physical protection systems
  - Computer management systems

- Systems and equipment require:
  - On-going consistent operation
  - Periodic maintenance
  - Modification and replacement
  - Occasional compensatory measures

✓ Security culture indicators

- Operation and maintenance use approved procedures
- Checklists and detailed procedures are used
- Compensatory measures are used when needed

Determination of Staff Trustworthiness

- Recognize any security system is vulnerable to insider assistance
- Trustworthiness determination process must be in place for all

✓ Security culture indicators

- Rigorous screening process that applies a graded approach and is capable of identifying specific risk factors matches risks and is documented and periodic
- Failures are appropriately investigated and adjudicated
- Staff members understand importance of trustworthiness
- Training in identifying high-risk behaviour
- Insider threat mitigation program is in place and well coordinated

Quality Assurance

- Important to ensuring security systems operate as designed
- Should be applied to all areas of security

✓ Security culture indicators
  - Assessment processes in place for security function
  - Staff understand that the management system is relevant to security

Change Management

- Many problems and failures in organizations are attributed to changes than can affect:
  - Equipment & Procedures
  - Organizational structures
  - Roles and responsibilities of personnel
- Must have effective processes to understand, plan, implement and reinforce changes

✓ Security culture indicators
  - Change management process in place for the security function
  - Changes are coordinated with all potentially affected organizations
  - Assessment made of changes to confirm desired outcome
  - Evaluations done at completion of change to see if it affected security

Feedback Process

- Organization must learn from itself and others
- Process for obtaining, reviewing, and applying experience from:
  - Internal sources
  - External sources

✓ Security culture indicators
  - Review national and international experiences
  - Allow and encourage reporting of abnormal events, concerns or near-misses
  - Actions taken to improve performance from experiences

Contingency Plans and Drills

- Be in continuous state of readiness
- Contingency plans must exist and be current
- Appropriate and realistic drills and exercises conducted of those contingency plans

✓ Security culture indicators
  - Contingency plans address design basis threat
  - Plans and staff are tested periodically through drills
  - All systems tested periodically, including seldom-used systems
  - Human factor in security systems is evaluated periodically

Self-Assessment

- Self-assessment includes wide variety of programmes, including:
  - Root cause analysis
  - Performance indicators
  - Lessons learned
  - Corrective action tracking

✓ Security culture indicators
  - Documented self-assessment programme and plan
  - Trends are identified and analyzed
  - Performances benchmarked against best practices
  - Operational performance is observed to confirm expectations
  - Corrective action plans developed and tracked

Interfaces

- Constructive, working relationship is important with regulator and law enforcement
- Information exchange is important to security

✓ Security culture indicators
  - Information freely and regularly exchanged
  - Vulnerability and threat information exchanged in timely manner
  - Regulatory interface roles are clearly defined

Coordination with Off-Site Organizations

- Off-Site intelligence interface is valuable
- Local and national police assistance and backup is necessary
- Written agreements and drills/exercises essential to assure coordination

✓ Security culture indicators

- Frequent communication with local and national security organizations
- Written agreements in place for assistance, communications, and timely response

Summary

- Management systems play a vital role in nuclear security culture
- Management system can affect the quality of work performed as well as the security needed to support it
- Management systems need to be visible and exercised

Small Group Exercise: Case Study #1

Management

Time: 20 minutes

Paul has seen Robert driving a new luxury sports car to work. Paul had recently heard Robert discuss some financial difficulties. Paul reports his concerns to management, but no action seems to have been taken.

Paul also observes his manager yelling at a co-worker who has reported a security concern. Paul is hesitant to report anything to his manager now and is not sure who to report his concerns to.

Small Group Discussion:

1. What are the good or bad indicator(s) of nuclear security culture in this case?

2. How would your facility address this scenario?

3. What improvements would enhance nuclear security culture in this case?

Small Group Exercise: Case Study #2

Management

Time: 20 minutes

Paul observes that the PTR facility manager is driving his vehicle into the PRN protected area. Because of his security training, Paul recognized the potential security risk of this behavior. He tries to discuss it with his manager and is told that it is one of the privileges of being a manager. Paul lets the matter drop.

Small Group Discussion:

1. What are the good or bad indicator(s) of nuclear security culture in this case?

2. How would your facility address this scenario?

3. What improvements would enhance nuclear security culture in this case?

Small Group Exercise: Case Study #3

Management

Time: 20 minutes

The manager notices that Alice, a material balance custodian, is routinely late for work. The manager asks Paul, who also works in the PTR, if he knows of a reason for this before confronting Alice. When the manager talks to Alice, she states she just doesn't like to be in the morning rush. However, after this meeting, he also notices that Alice appears to be taking long lunches and tends to leave before her coworkers. He decides that disciplinary actions are needed. During subsequent meetings, Alice states how important she is to facility operations and jokes that she must might take some material.

Small Group Discussion:

1. What are the good or bad indicator(s) of nuclear security culture in this case?

2. How would your facility address this scenario?

3. What improvements would enhance nuclear security culture in this case?

Small Group Exercise: Case Study #4

Management

Time: 20 minutes

Paul has successfully been promoted to manager and now has greater access to nuclear operations. This promotion comes with more responsibility. However, he notices that his staff still treat him like a coworker and are asking him for favors such overlooking forgotten badges and tardiness.

Additionally, Paul has noticed several potential security issues. He is concerned in his new role, that fixing these security issues might negatively affect operations.

Small Group Discussion:

1. What are the good or bad indicator(s) of nuclear security culture in this case?

2. How would your facility address this scenario?

3. What improvements would enhance nuclear security culture in this case?

Nuclear Security Culture

End of Career

Retirement and Termination

Partnership for Nuclear Security

National Nuclear Security Administration

Phases of Employment

- Hiring
- On the job
- Transfers within the company
- End of employment (usually referred to as "termination")

Personnel Termination Reasons

- Normal Attrition
  - Changes in jobs
  - Relocation
  - Layoff
  - Retirement
  - Death
- Termination for Cause

Security Implications

- Revocation of all access
  - Computer
  - Physical
- Return or transfer of all
  - Property
  - Documents
  - Data
- Non-disclosure agreement

These actions must be taken immediately upon termination!

Determining When Disciplinary Action Is Needed

- Misdeed is discovered
  - Reported by another employee
  - Observed by manager
  - Misdeed is sensed by security or safety system
- How does case get adjudicated or decision to fire employee made?
- How much time before decision is implemented?

Termination Action Issues

- Employee should not be allowed back to workstation unescorted
  - To pick up personal effects
  - Never left unattended
- Use configuration management to monitor tasks to prevent unapproved changes to mission critical systems
- Are there other measures that could be done?

Layoffs

- Is the employee expected to come back?
- After how much time?
- Will accounts and access be dormant or terminated?
- Do termination actions apply?
- What would be different?

Summary

- Nuclear security culture applies throughout an employee's career
- Security must be considered no matter how the employee terminates employment
- In some cases, preventative measures are needed to pre-empt malicious acts

Small Group Exercise: Case Study

Termination – Firing

Time: 20 minutes

Brian is a system administrator who was angered by his job performance review, feeling that his work was not valued. He was responsible for the computer networks at the facility. Frustrated, Brian intimidated a coworker into giving him the only backup tapes for the company proprietary software used to support the control systems at the PTR.

The coworker reported Brian for inappropriate and abusive treatment of his coworkers. As a consequence, Brian was terminated. After his termination, a logic bomb that Brian previously planted detonated, deleting the only remaining copy of the critical software from the company's server.

Small Group Discussion:

1. What are the good or bad indicator(s) of nuclear security culture in this case?

2. How would your facility address this scenario?

3. What improvements would enhance nuclear security culture in this case?

Small Group Exercise: Case Study

Termination – Firing
Time: 20 minutes

Brian is a system administrator who is under contract to maintain the Lagassi facility computers and control systems. It was against Lagassi policy, but Brian chose to do similar work on the side for his own business and conducted some of that business while at the Lagassi facility. Brian's activities were discovered and management met with Brian to discuss his violation of company policy and his termination. This meeting went well and Brian admitted his mistake and offered a heartfelt apology for having caused this uncomfortable situation. The managers were relieved that the meeting had gone well and told Brian that he could retrieve his personal gear from his office and his computer, then hand in his keys and badge on this way out. However, Brian used his high-level admin passwords and connected to every Lagassi server. He formatted every drive on the server, including the backup systems. Then, he grabbed his cardboard box of books and family pictures and walked to the door with a smile.

Small Group Discussion:

1. What are the good or bad indicator(s) of nuclear security culture in this case?

___

___

___

2. How would your facility address this scenario?

___

___

___

3. What improvements would enhance nuclear security culture in this case?

___

___

___

Small Group Exercise: Case Study

Termination – Retirement

Time: 20 minutes

Paul has made it to retirement age. He is feeling pressure from upper management to retire to "make room for the younger generation". He knows this is about budget and resents the pressure from management. He sees his job assignments dwindling and recognizes how this will affect his performance review.

Paul gets tired of the politics and decides to retire. Everyone is happy for him and he puts on a good face. However, while cleaning out his office, he decides to shred all of his files rather than transfer them to someone else. These files include results of vulnerability analyses need for an upcoming audit and trends analysis indicating a failure of the PTR sensor system is imminent. He thinks "Let them deal with that without me!"

On his last day, Paul enjoys his party knowing he left the facility with some major problems to deal with.

Small Group Discussion:

1. What are the good or bad indicator(s) of nuclear security culture in this case?

2. How would your facility address this scenario?

3. What improvements would enhance nuclear security culture in this case?

Small Group Exercise: Case Study

Termination – Layoff

Time: 20 minutes

Paul has enjoyed working for LMRI. However, due to government budgetary issues, the LMRI must reduce staff until the budget is resolved. Since the PTR where Paul works is the primary cost element at LMRI, the staff at the PTR are being laid off. All are assured that there jobs will continue when the budget is resolved. Because of this, all staff will keep their badges in the belief that the layoff will be short in duration.

Paul and his wife just had their fourth child and his ailing mother-in-law has come to live with his family. This wasn't a good time for a layoff!

Small Group Discussion:

1. What are the good or bad indicator(s) of nuclear security culture in this case?

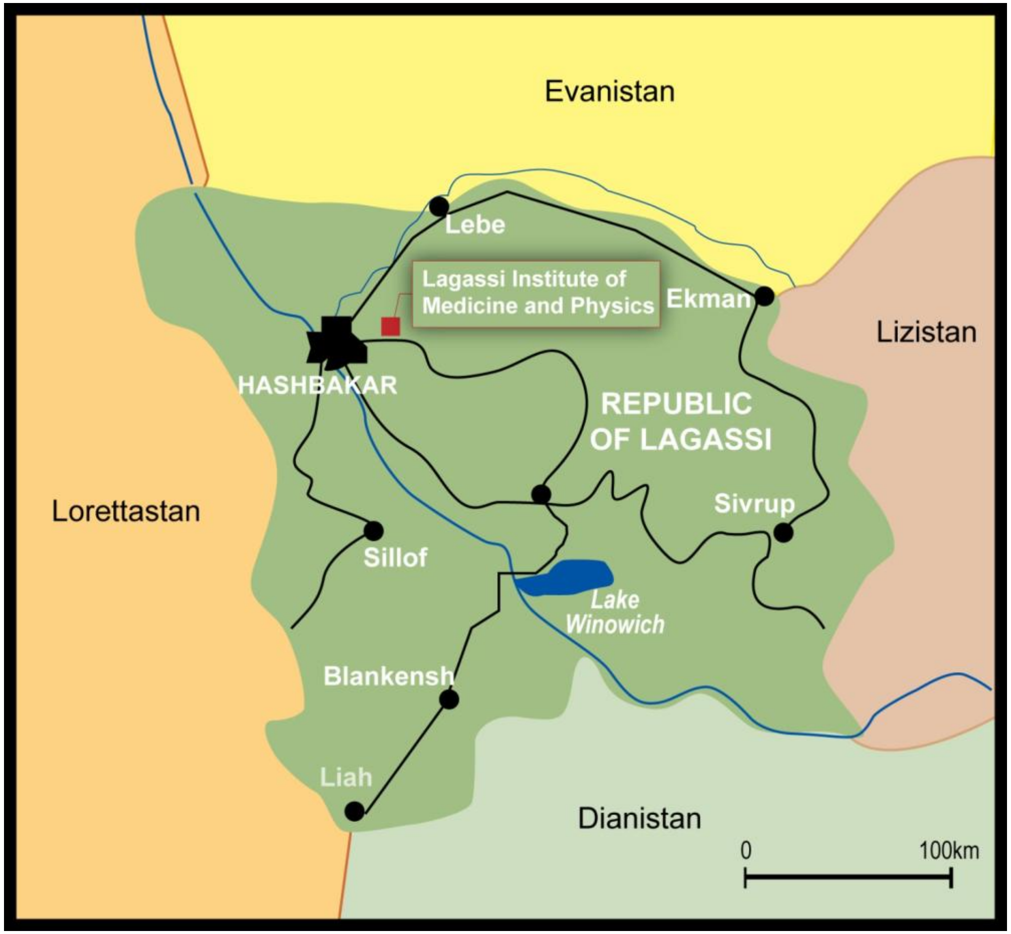
2. How would your facility address this scenario?

3. What improvements would enhance nuclear security culture in this case?

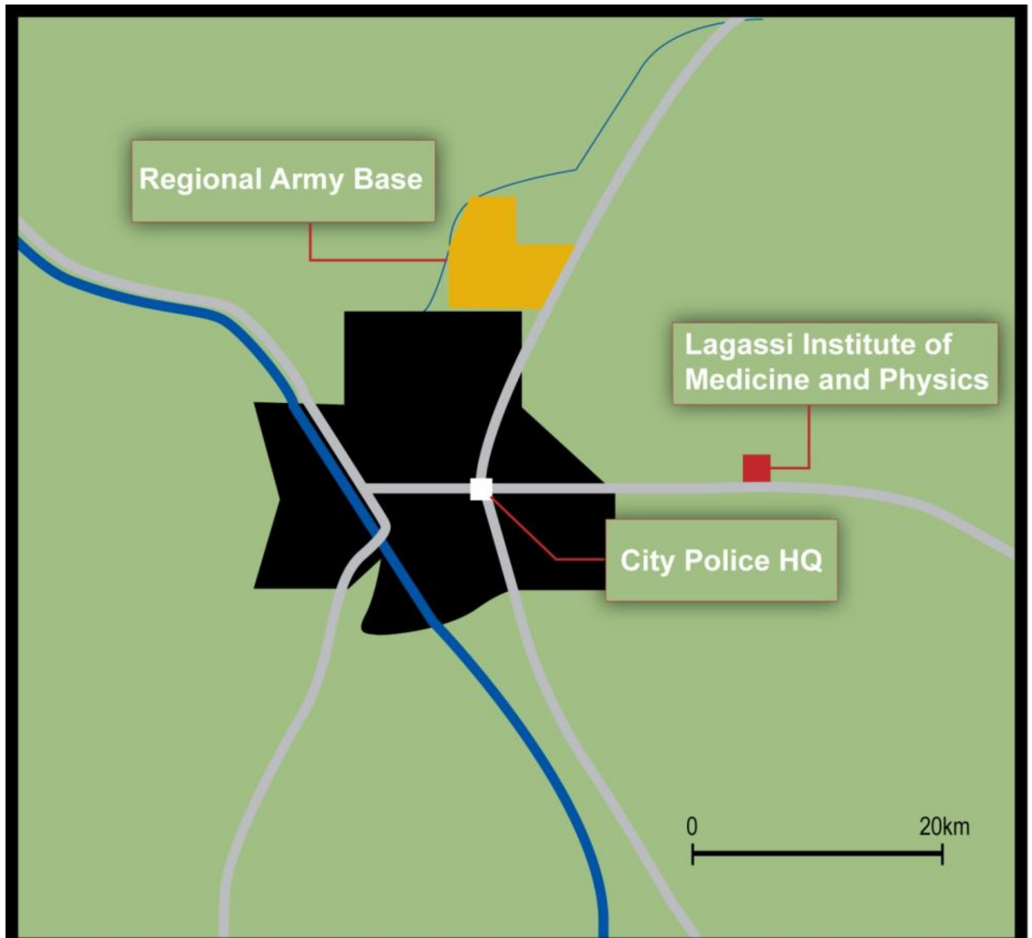
Nuclear Security Culture

Introduction to Lagassi

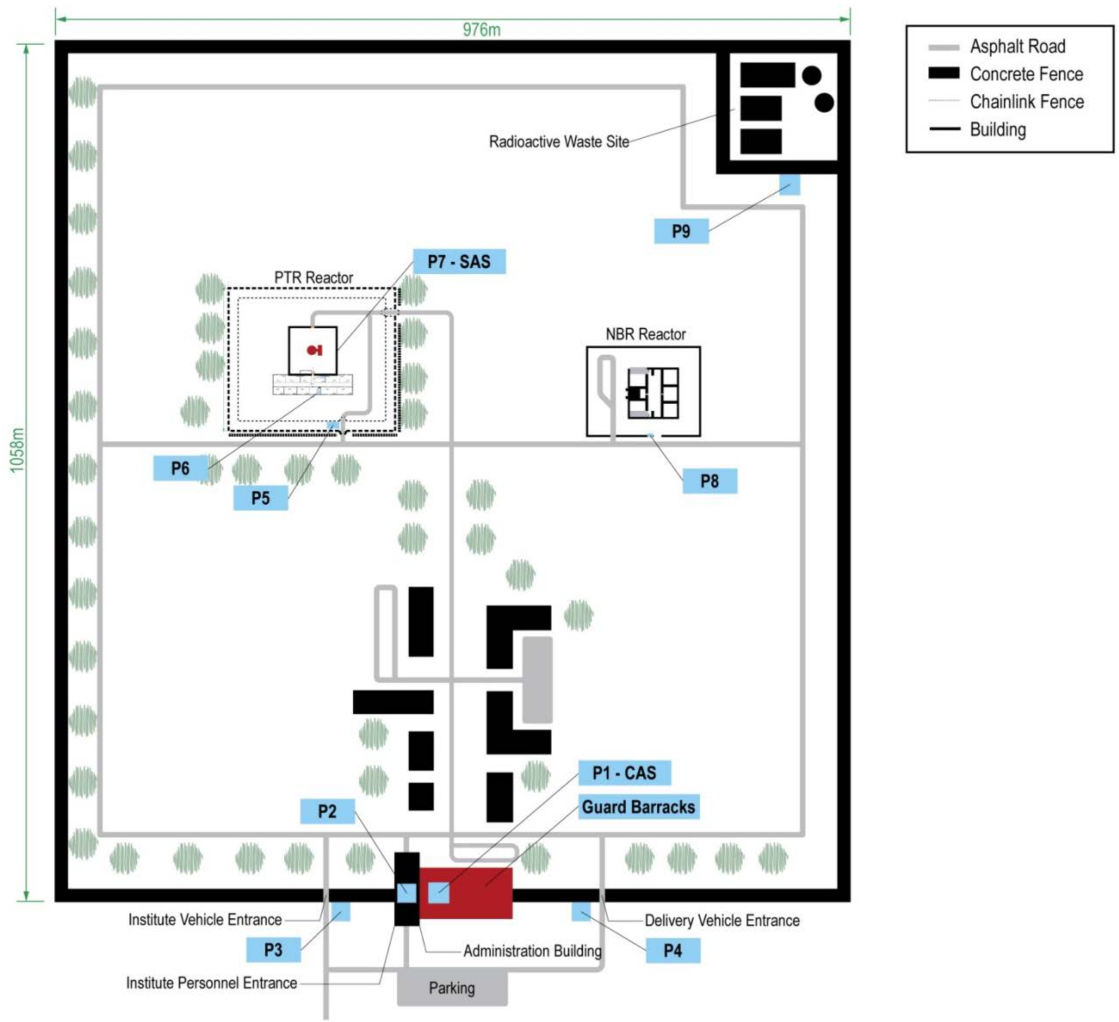
Country of Lagassi



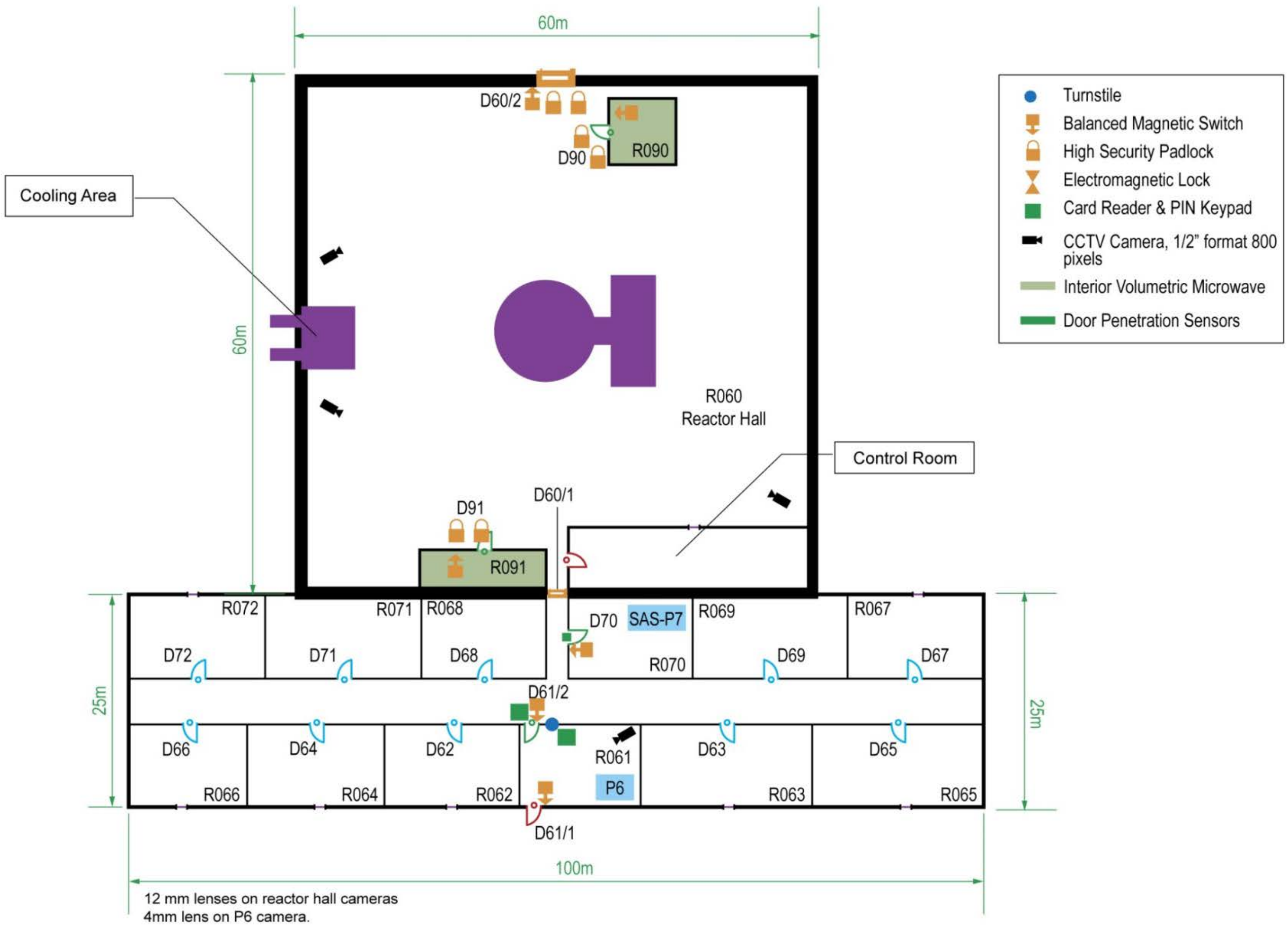
Lagassi Institute of Medicine and Physics



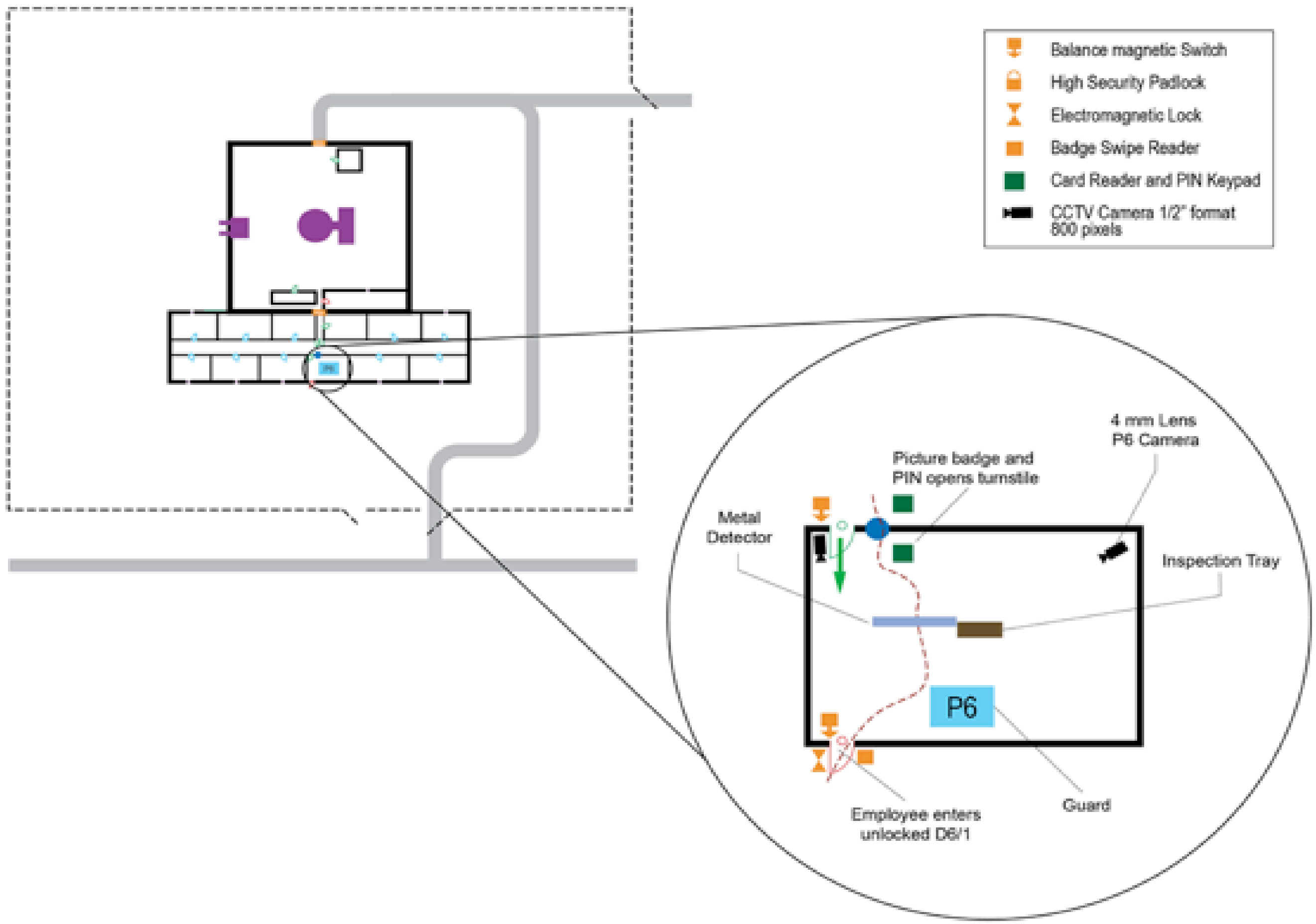
LNRI Hypothetical Facility



PTR Research Reactor – Building Floor Plan



PTR Access Plan



Employees with PTR Access

- LNRI Plant Manager
- Shift Supervisor
- Reactor Operators
- Operations Support
- Maintenance Manger
- Electrical Maintenance
- Mechanical Maintenance
- Administrative Support
- Health Physics Technicians
- Vendors
- Lagassi Safety/Security Inspectors
- Janitorial Staff
- Material Balance Custodians
- Nuclear Material Technicians
- Nuclear Material Accountability Technicians
- Engineering Support
- Safety Engineers
- Security Analyst
- Guard Supervisor
- Alarm Station Operators
- Patrol Guards
- Post Guards

Exercise Data Book
for the
General Hypothetical Facility
and
PTR Data

Table of Contents

Lagassi **6**

The City of Hashbakar **7**

The Lagassi Nuclear Research Institute **8**

The Pool-Type Reactor (PTR) 8
The Waste Storage Site 8

LNRI Hypothetical Facility **9**

Physical and Environmental Conditions near the LNRI **10**

Topography 10
Vegetation 10
Wildlife 10
Background Noise 10
Climate/Weather 10

PTR Research Reactor General Description **11**

Reactor Data 11
Cooling System 11
Irradiated Fuel Storage and Handling 12
Fresh Fuel Storage and Handling 12
Experiment Materials 12

Nuclear Material Stored or In Use at the LNRI **13**

Intelligence Sources from the National Government 14
Crime Study 14
Professional Organizations 14
Site-Specific Data 15

Response Force Data **16**

Types of Guard Force Personnel 16
Responsibilities of Institute Guards 16
Local Police Patrols 16
Military Tactical Response Team Members 16
Equipment .... **Error! Bookmark not defined.**
Training .... **Error! Bookmark not defined.**
Alarm Stations and Communication (P1) .... **Error! Bookmark not defined.**
Response Force Staffing 17
Response Procedures 18
Facility Entry Control Operations at LNRI Gates and Portals 19
Institute Personnel Entrance (P2) 19
Institute Vehicle Gate (P3) 19
Institute Delivery Vehicle Gate (P4) 20

Entry Control Procedures for the PTR Facility **21**

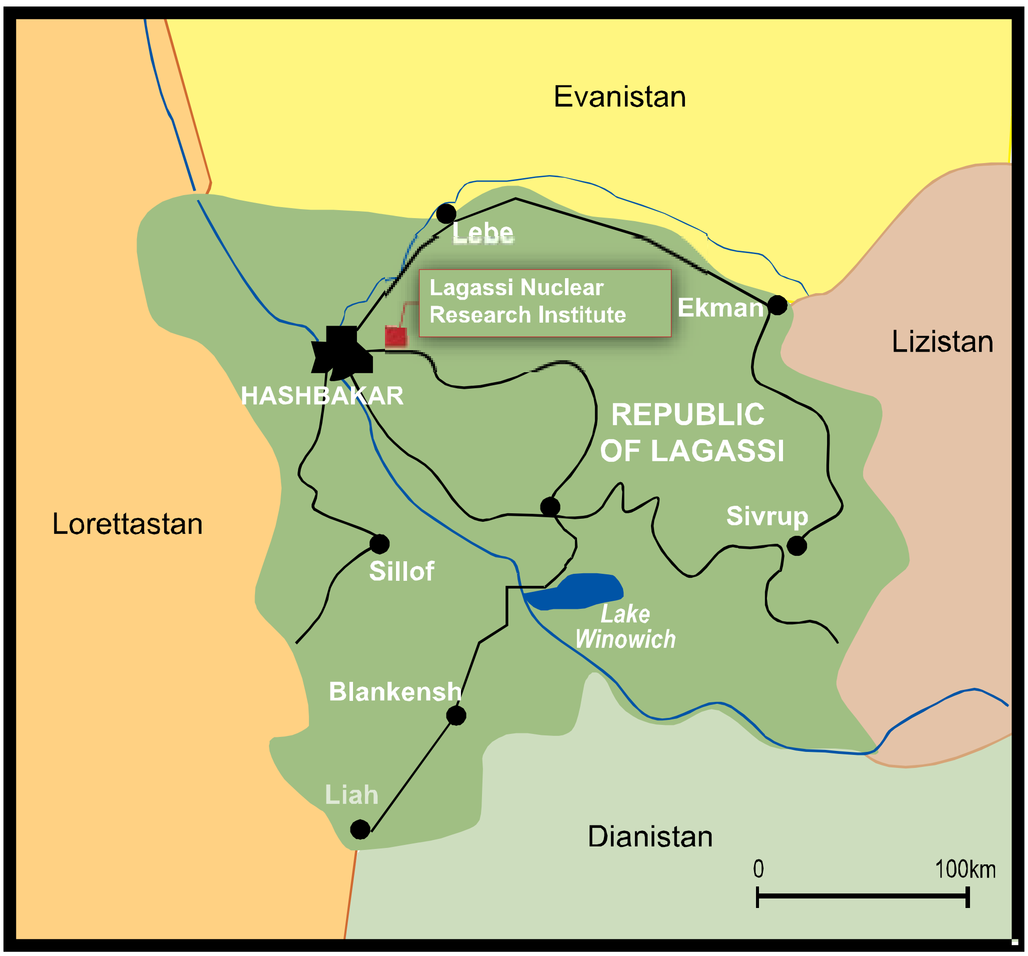
PTR Personnel and Vehicle Gates (P5) 21
PTR Building Personnel Portal (P6) 21
PTR Emergency Vehicle Portal (P8) 22
PTR Research Reactor – Building Floor Plan 23
PTR Interior Physical Protection Elements 24

25
Personnel..26

Lagassi

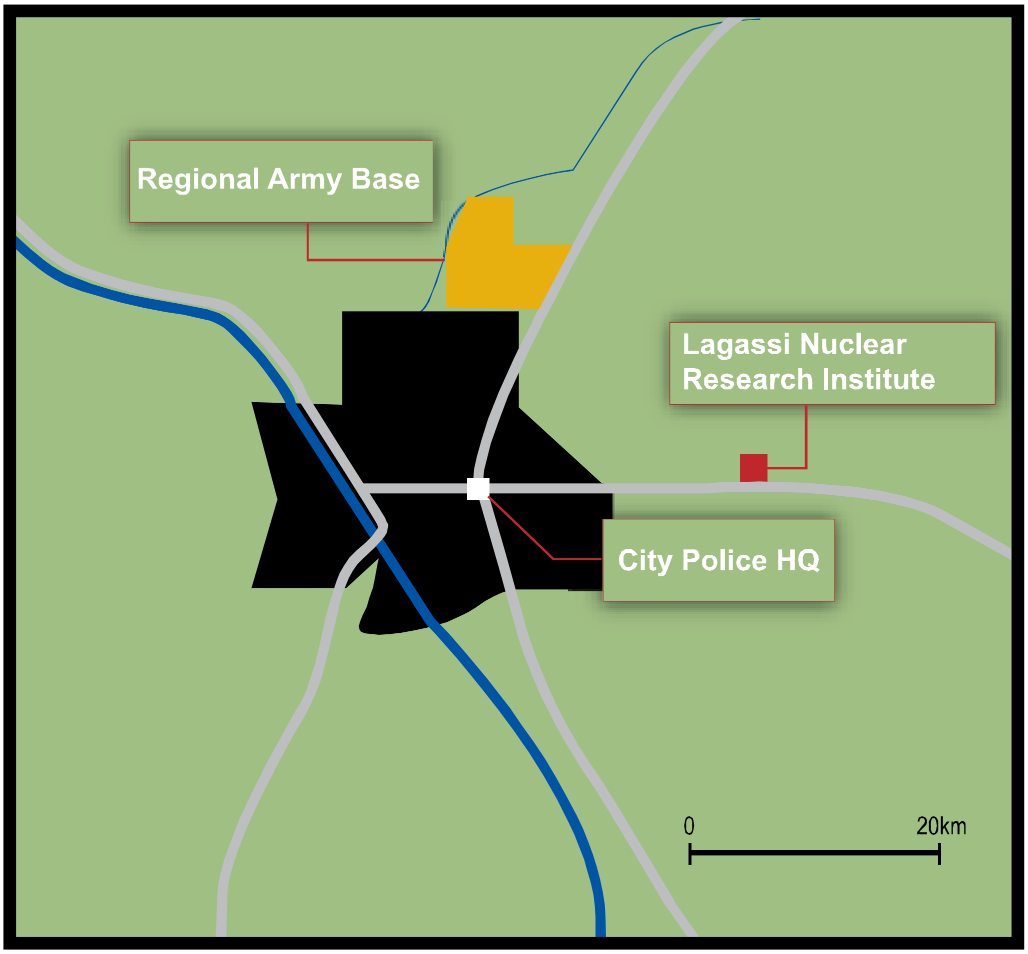
Lagassi, the smallest of the regional republics, possesses large fossil fuel reserves and plentiful supplies of other minerals and metals. It also has a large agricultural sector featuring livestock and grain. Lagassi's industrial sector rests on the extraction and processing of these natural resources and also on a growing machine-building sector that specializes in construction equipment, tractors, agricultural machinery, and some defense items. The country's solid 3.5% economic growth is largely due to its booming energy sector, but also to economic reform, good harvests, and foreign investment. In order to prevent overdependence on the oil sector, the country has embarked on an industrial policy designed to diversify the economy by developing light industry and a nuclear energy infrastructure.

Current issues include expanding the development of the country's emerging nuclear energy resources, achieving an export capacity of electrical energy to border countries, and strengthening relations with neighboring states and other foreign powers.



The City of Hashbakar

The capital of Lagassi is Hashbakar, an ancient city that arose from the crossroads of early trading lanes. Today, the city is a modern metropolis of two million inhabitants. The city contains a major roadway, a rail system, a private and military airport, and a limited waterway.



The Lagassi Nuclear Research Institute

The (hypothetical) nuclear research center, Lagassi Nuclear Research Institute (LNRI), was started in 1950 to serve as the nation's premier nuclear energy research facility. The Institute houses various research, administrative, and plant support facilities. The LNRI is located in the Republic of Lagassi, approximately 29 km (18 mi) east of Hashbakar.

The Pool-Type Reactor (PTR)

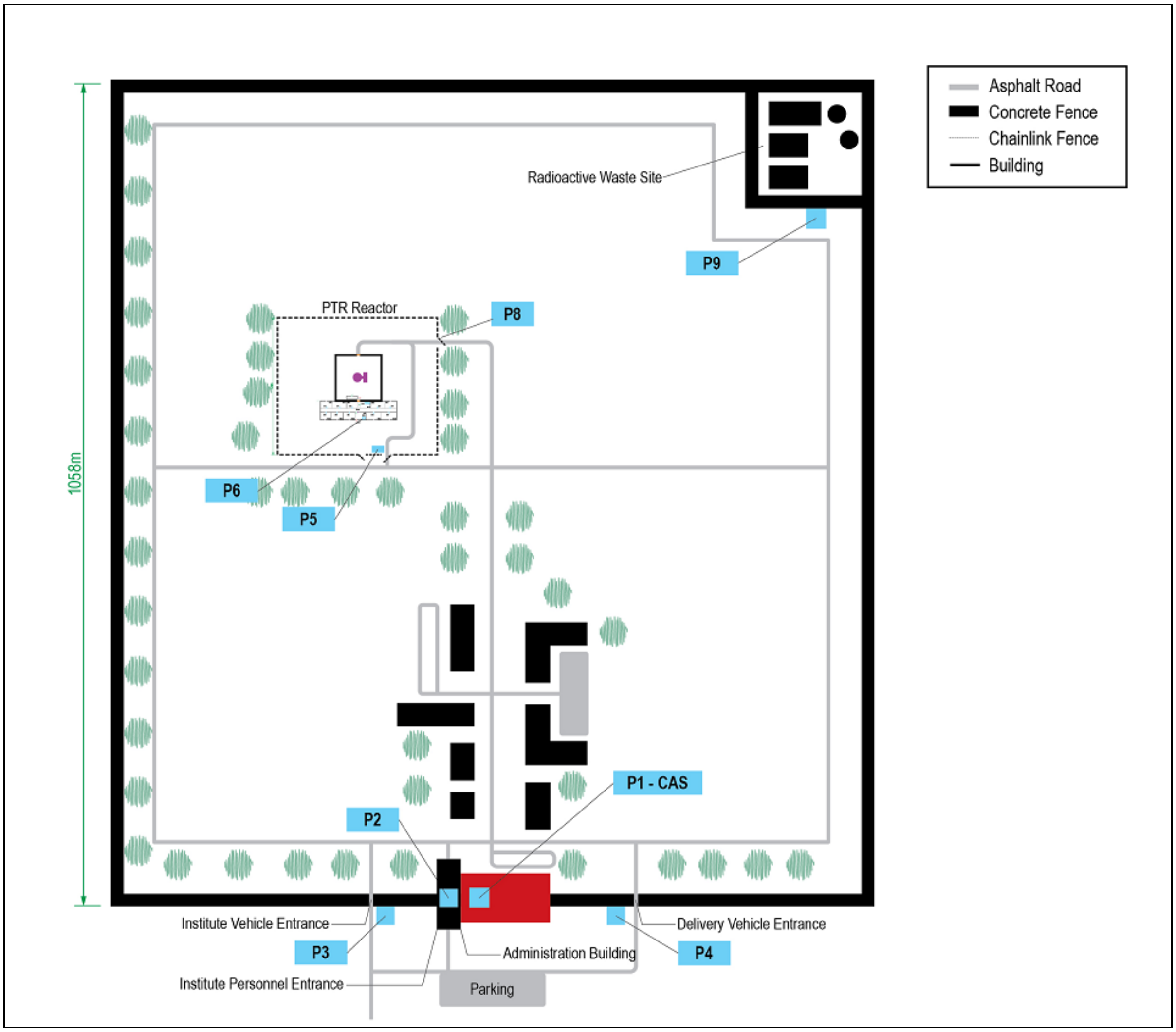
LNRI has a facility that houses a light-water moderated, highly enriched uranium (HEU)-fueled research reactor, which is considered a pool-type reactor (PTR). The PTR is used for research on advanced reactor components, special fuel assemblies, and production of radionuclides for the medical industry. Other experiments are performed to investigate power reactor fuel when heated to the point of melting.

The PTR Research Reactor facility employs a total of 32 people, plus the guard force. The reactor is not usually operated during the evening and off-shifts. During the off-shift periods, the gates to the facility and doors to the PTR Building are locked and alarmed.

The Waste Storage Site

The Waste Storage Site is located at the northeast corner of the LNRI. The Waste Storage Site is an IAEA Category III site that is used for the storage of radioactive wastes from the PTR and other institute facilities. The site contains an unloading structure, a storage area for low-level liquid wastes, a burial area for wastes mixed with concrete, and storage buildings for medium-level and high-level wastes, isotopes, and metals. Because of recent theft attempts by local civilians and a group of students, all of whom were contaminated during these attempts, the site is now under 24-hour guard. The medium-level and high-level metals and isotopes are the main concern of the LNRI safety and health physics personnel.

LNRI Hypothetical Facility



Legend:

P1 = Central Alarm Station (CAS)
P2 = Institute Personnel Entrance
P3 = Institute Vehicle Gate
P4 = Institute Delivery Vehicle Gate
P5 = PTR Personnel Gate
P6 = PTR Entry Control Portal and Secondary Alarm Station (SAS)
P8 = PTR Emergency Gate
P9 = Radioactive Waste Site Guard Post

Physical and Environmental Conditions near the LNRI

Topography

The LNRI is located in a semi-arid environment.

Vegetation

Small shrubs, cacti, hardy desert trees, and sparse grass are the only vegetation in the area.

Wildlife

Small animals such as rabbits, squirrels, prairie dogs, and coyotes inhabit the area. Birds of all sizes are also present.

Background Noise

Regional earthquakes cause seismic disturbances occasionally. Some noise may also occur because of heavy passenger vehicle traffic on nearby roads and low-flying aircraft.

Climate/Weather

The climate is a typical high-desert environment with approximately 300 clear days of bright sunshine per year. On cloudy days, there are areas with a high light-to-dark ratio because of moving cloud shadows. Rainfall is about 15 cm per year, with the majority occurring during seasonal thunderstorms in the late July–August rainy season. The spring is typically very windy for two to three months, with continuous winds of 2 to 5 km/hr and gusts up to 50 km/hr. Dry debris, dust, and dead vegetation are blown about during the windy season.

PTR Research Reactor General Description

The PTR, our hypothetical facility, is a light-water moderated, highly enriched uranium (HEU)-fueled research reactor located within the Lagassi Nuclear Research Institute (LNRI), a hypothetical nuclear research center. The LNRI is located in the Republic of Lagassi, approximately 29 km (18 mi) east of the capital city of Hashbakar, the major population center.

The reactor is used for research on advanced reactor components, special fuel assemblies, and production of radionuclides for the medical industry. Other experiments are performed to investigate power reactor fuel when heated to the point of melting.

Reactor Data

- The pool-type research reactor is used in a steady-state operation of 2 MW. The continuous operation cycle is 14 days.
- The irradiation cavity is a 23 cm diameter dry tube in the center of the reactor.
- The annular core is formed by 236 cylindrical fuel elements arranged in a hexagonal grid around the central irradiation cavity.
- The reactor is controlled by seven fuel-followed control rods with rod drive motors accessible.
- At least five control rods must be removed for the reactor to go critical.
- Fuel material is BeO-UO_2, 22 wt% UO_2, 78 wt% BeO with uranium enriched to 36 percent.
- Each fuel element is approximately 1 meter long, 2 cm in diameter, and weighs a total of 2 kg.
- Each fuel element contains 103 grams of ^{235}U and is clad in stainless steel.
- Fuel rods are placed in a grid and may be removed with a rigid fuel-handling tool.
- Centerline fuel temperatures range up to 1,500°C.
- Water serves as coolant and moderator. The core is located in an open pool 3.1 meters in diameter and 8.5 meters deep.

Cooling System

- The pool contains 62.5 cubic meters of deionized water at a maximum temperature of 60°C.
- The core is cooled by natural convection in the water pool.
- The pool is constructed of stainless steel.
- A forced air/water heat exchanger is used to discharge the waste heat to the atmosphere.
- The heat exchanger is inside the reactor building with air ducts (and grids) through the building walls.
- The air ducts are mild steel, 0.3 cm thick, and has a grill that is #4 (13 mm) rebar on 15 cm centers.

- The reactor core is designed so that if a complete loss of water occurs after sustained 2-MW operation, air is sufficient for cooling. (However, natural circulation of air is essential.)
- Pumps are located below the reactor coolant level to ensure adequate Net Positive Suction Head.
- The cleanup loop flow rate of 1 to 2 liters/sec is used to:
  - remove impurities
  - maintain pH
  - maintain resistively within specifications
  - provide deionized makeup water

Irradiated Fuel Storage and Handling

- Irradiated fuel elements are transferred underwater to the spent fuel storage pools.
- The elements are transferred in storage racks using rigid handling tools.
- The dose rate of freshly discharged spent fuel is approximately 0.2–0.3 SV/hr. (20–30 rem/hr) at 1 meter.
- There are currently 100 irradiated fuel rods in the spent fuel storage pools.

Fresh Fuel Storage and Handling

- Fuel rods arrive in shipping containers.
- Fuel rods are stored in a reinforced concrete storage vault, R090, in the reactor building.
- Fuel storage racks capable of holding 10 fuel rods are used to transfer new fuel rods into the reactor pool.
- The storage vault can hold five storage racks.
- Cotton gloves are worn when directly handling the fuel rods.
- A rigid fuel-handling tool is used to transfer the fuel storage racks to its intended position once in the reactor pool.
- Currently, there are 50 fresh fuel rods (5 full storage racks) in storage.

Experiment Materials

- Experiment materials include 3 kilograms total of highly radioactive medical radionuclides, including Cs, Am, and Sr^{90}.
- A maximum of one assembly of mixed oxide fuel rods is in the reactor core at any one time and no more than four are located on site at one time. Each MOX assembly weighs a total of 3 kg and each contains 2 kg of $plutonium^{239}$.
- Other sources are used in other irradiation and activation experiments.

Nuclear Material Stored or In Use at the LNRI

Table 1. LNRI Nuclear Material

Facility	Location	Form of Material	Amount of Material On Site (wt% enrichment)	Total Isotope Amounts	Level of Radiation
PTR Research Reactor	Reactor	BeO-UO_2 Fuel Rods (236 in reactor)	67.5 kg U (36%)	24.3 kg ^{235}U	High >1 Gy/hr at 1m
	R090 Fresh Fuel Vault	BeO-UO_2 Fresh Fuel Rods (50 in storage)	14.3 kg U (36%)	5.2 kg ^{235}U	Low
	Irradiated Fuel Pool	BeO-UO_2 irradiated fuel Rods (100 in pool)	28.6 kg U (35%)	10.0 kg ^{235}U	High 0.2–0.3 Gy/hr at 1m
	R091 Product Vault	Pu Experiments HEU metal Other Sources	9.3 kg $^{239}PuO_2$ (100%) 23 Kg U (95%) Cs, Am, Sr	8kg 22 Kg ^{235}U 3 kg total	Low Low High
Waste** Storage Facility	Vats (Large tanks for Liquids)	Liquid Mixture (4 vats, 1,000 liters ea)	Trace Amounts* of Pu (75%) and U (18%) Co, Cs	trace	High 0.5–1 Gy/hr at 1m
	Sheds	Solidified Waste (50 containers)	Trace Amounts* of Pu (31%) and U (12%)	trace	High <0.5 Gy/hr at 1m

**The term “trace amount” refers to an extremely small amount in quantities approaching the limit of detection for the analytical process used to characterize the material.*

*** Waste is defined as radioactive material for which there is no further use. For Lagassi, this material is still under regulatory control and is protected according to prudent management practice.*

Threat Data

Intelligence Sources from the National Government

- Items were recently confiscated from a political terrorist group's hiding place, which was located less than 200 km from the LNRI. The items included internal engineering drawings of the LNRI with circles drawn around the PTR Reactor and the waste storage; various weapons, including automatic weapons; some explosives; and evidence of correspondence and communication with a foreign terrorist group. Interviews with property owners and residents indicated the group consisted of three to five men.
- Surveillance of several suspected members of the terrorist group shows extensive travels in and out of the country.
- The economic and civil strife in a neighboring country has caused many refugees, some of which are suspected terrorists, to enter Lagassi illegally.
- Plans by a political terrorist group to attack shipments of nuclear material in a neighboring country were discovered.
- The local police intelligence reports state that several Special Forces members had been offered large cash payments to provide special training to unidentified individuals.
- The national intelligence organization reports terrorist groups are operating in cells of four to six individuals and compartmentalizing information.
- A group of international terrorists made threats that they have the ability (skilled members and weapons) to take over or create a radiological release of a foreign nuclear facility. They demanded the release of several political prisoners. Investigation proved that they do have the weapons and equipment they claimed they have.

Crime Study

An analysis of crime incidents leads to the following conclusions:

- A major bank robbery was committed in the capital two months ago. Four robbers escaped with a large amount of money. Investigation shows the bank vault was breached by the sophisticated use of high explosives stolen from the local army base. [Note: the crime of robbery includes use of weapons.]
- Nationally, many thefts of highly valuable items have occurred. The crimes do not appear to be related to each other. National intelligence information indicates that, most likely, several groups committed the crimes. Organized crime may be involved.

Professional Organizations

- A recent meeting of the Lagassi Atomic Energy Ministry included a special session on analysis of threat to nuclear facilities and material. No substantiated data on threat were available. However, the general feeling among members was that a threat to nuclear facilities does exist.
- During a meeting of the Industrialists Society, some corporate managers expressed concern that some of their employees had been approached by unnamed groups to help them carry out theft of valuable equipment and materials from the corporations. The employees had been offered large amounts of money.

Site-Specific Data

- An analysis of the backgrounds of the employees of LNRI and of the population of the community did not provide any information that would suggest a concern of threat to the Institute.
- There have been no serious disputes over labor issues at the LNRI in the past five years.
- Local news media publicized that the security system at the LNRI was the latest in modern security system design with full IAEA compliance.
- A recent news feature raised the question of the potential risk to public health of the many radiological isotopes present in the LNRI.
- An Institute employee was recently caught stealing equipment and was terminated from the facility.
- A site-wide inventory recently discovered that several controlled site drawings were missing.

Response Force Data

Types of Guard Force Personnel

The guard force consists of three types of security personnel:

- Unarmed institute guards
- Local armed police patrols
- Military tactical response teams

Responsibilities of Institute Guards

These security personnel are responsible for:

- Assessing alarms
- Performing administrative duties, such as access control and key service
- Staffing fixed posts and patrols
- Responding to all assessed intrusion alarms (non-confrontation)
- Observing adversary actions and communicating them to the alarm station

All posts and patrols have defined policies and procedures with which the security personnel must comply.

A supervisor is present for each shift for the institute guards that conduct administrative duties and access control.

Local Police Patrols

Each local police patrol consists of two police officers in a patrol car. They are responsible for protecting the neighborhood around the LNRI, including the facility. There are two patrols in the area outside the LNRI 24 hours a day. They are responsible for:

- performing random status checks with either the P2 or P3 guard a minimum of three times per day.
- responding to assessed intrusion to delay intruders until the military tactical response team arrives

They are not trained to enter the reactor buildings.

Military Tactical Response Team Members

There are two military tactical response teams on 24-hour alert. The teams have five members each. All members are trained in hostage situations and close-quarters combat, and have the authority and training to ensure the safety of critical assets and target material. However, they have never entered the PTR facility, nor do they have keys or breaching equipment to do so.

Response Force Staffing

The response force posts and patrols are staffed as described in the following tables.

Table 2. Guard Staffing Data

Post No.	Description	Security Personnel Type	No. of Personnel	
			Day Shift	Nights and Weekends
P-1	CAS (includes commander)	Guard	2	1
P-2	Institute Personnel Entrance	Guard	2	1
P-3	Vehicle Entrance (Main Gate)	Guard	1	0
P-4	Delivery vehicle entrance (Main Gate)	Guard	Unmanned	Unmanned
P-5	PTR Personnel and vehicle gate	Guard	Unmanned	Unmanned
P-6	PTR Building Personnel Portal	Guard	1	0
P-8	PTR Emergency Vehicle Portal	Guard	Unmanned	Unmanned
P-9	Radioactive Waste Site entrance	Guard	1	1
P-10	Random two-man patrol of Institute	Guard	2	2
		Totals	**9**	**5**

Table 3. Police Patrol Staffing Data

Post No.	Description	Security Personnel Type	No. of Personnel	
			Day Shift	Nights and Weekends
	Two-person patrols in local area	Police patrol units	4	4
		Totals	**4**	**4**

Table 4. Military Tactical Response Staffing Data

Post No.	Description	Security Personnel Type	No. of Personnel	
			Day Shift	Nights and Weekends
	Military tactical response teams (two teams of five personnel each)	Tactical Teams	10	10
		Totals	**10**	**10**

Response Procedures

All intrusion alarms are received at the CAS. Upon receipt of an alarm, the CAS operator manually calls up the video from the appropriate camera. When video assessment is not available, the CAS operator notifies the roving patrol (P-10) to visually assess the cause of the alarm. If assessed as an intrusion, the CAS operator notifies the local police dispatcher, who then notifies the local police patrols to respond to the LNRI. The CAS operator then notifies the Commander of the military tactical response unit in order for the appropriate tactical team to begin preparations for deployment.

The CAS then notifies the guards to initiate actions designed to protect employees by warning them, evacuating them when appropriate, and performing other actions that might obstruct the adversary (locking doors, disabling power, etc). Under no circumstances are the guards to approach or engage the adversaries.

When the first police patrol arrives at the entrance to the LNRI, the officers receive a quick briefing from the guard supervisor, and then begin to tactically assess the situation. Upon arrival of the second patrol, the two patrols deploy to *contain* the adversary and prevent employees from becoming injured.

Once the military tactical team arrives at the LNRI, the team receives a status briefing from the guard supervisor and receives an institute radio. The guard supervisor and tactical team leader coordinate entry with the guards and deploy as appropriate to ensure the protection of material and assets.

Facility Entry Control Operations at LNRI Gates and Portals

Institute Personnel Entrance (P2)

During normal working hours entrance is controlled by two guards. One guard is inside the P2 at all times. During off-shift hours, the personnel entrance is locked with one guard present.

Entry Procedures

- Personnel form a single line and show the guard their badges as they enter.
- Personnel enter through the front door of the Administration Building and continue out the back of the building to go to other areas in the facility.
- The guard observes personnel for unusual behavior.

Exit Procedures

- Personnel form a line inside the Administration Building.
- The guard waves personnel to pass one at a time out the front door.
- The guard observes personnel for unusual behavior.

Institute Vehicle Gate (P3)

During normal working hours the gate and associated traffic flow are controlled by a single guard. The gate is unlocked and open during normal working hours and locked during off-shifts. During normal working hours, site vehicles (designated by special markings on vehicle) and the automobiles of authorized employees (designated by special marking on personnel badge) are allowed entry through the gate.

Entry Procedures

- Drivers form a single line, approach the vehicle gate slowly, then stop to show the guard their badges as they enter.
- The guard verifies the vehicle and driver is approved into the facility by checking markings and badges of all passengers, if authorized, the unarmed guard waves the driver to pass into the facility one at a time.
- The guard observes the drivers and passengers for unusual behavior.

Exit Procedures

- Drivers form a line inside the facility and when directed by the guard, slowly approach the vehicle gate.
- The guard waves drivers to pass one at a time out of the facility
- The guard observes drivers and passengers for unusual behavior.

Institute Delivery Vehicle Gate (P4)

This gate is normally closed and locked with a high security padlock. A guard is not typically on post. The second guard at the Personnel Entrance is dispatched to open the gate for announced deliveries and emergency evacuations.

Entry Control Procedures for the PTR Facility

PTR Personnel and Vehicle Gates (P5)

These gates are opened at 0600 and closed at 1800 and guard sare not present. A guard is required to open the gates after hours.

PTR Building Personnel Portal (P6)

The Building Personnel Portal is staffed by one guard during normal working hours. During off-shift hours, the doors are locked and the guards are not present.

Entry Procedures

1. The employees enter through the unlocked outer door one at a time.
2. Each person presents his picture badge to the guard.
3. If the picture on the badge and the person's face match, the guard directs the person through the metal detector.
4. If the person is carrying or transporting a package, the guard observes the package.
5. If the package looks suspicious, the guard inspects the package.
6. Under the observation of the guard, the person, with any packages, walks through the metal detector.
7. If there is an alarm, the guard performs an inspection of the person and package.
8. If there is no alarm or the person and package is cleared by the guard, the person continues to enter the building.
9. Once past the metal detector, the employee scans his badge and enters his personal identification number (PIN).
10. If the PIN is correct, the turnstile becomes operable and allows entry into the building.
11. The guard allows the next employee to enter.

Exit Procedures

1. The employees line up to enter the portal through the locked door one at a time.
2. The first person scans his badge and enters his PIN.
3. If the PIN is correct, the door opens, allowing him to enter the portal.
4. If the person is carrying or transporting a package, the guard observes the package.
5. If the package looks suspicious, the guard inspects the package.
6. Under the observation of the guard, the person, with any packages, walks through the metal detector.
7. If there is an alarm, the guard performs an inspection of the person and package.

8. If there is no alarm or the person and package is cleared by the guard, the person exits the portal.

PTR Emergency Vehicle Portal (P8)

The Emergency Vehicle Portal is staffed by response force staff only in times of emergency or special use.

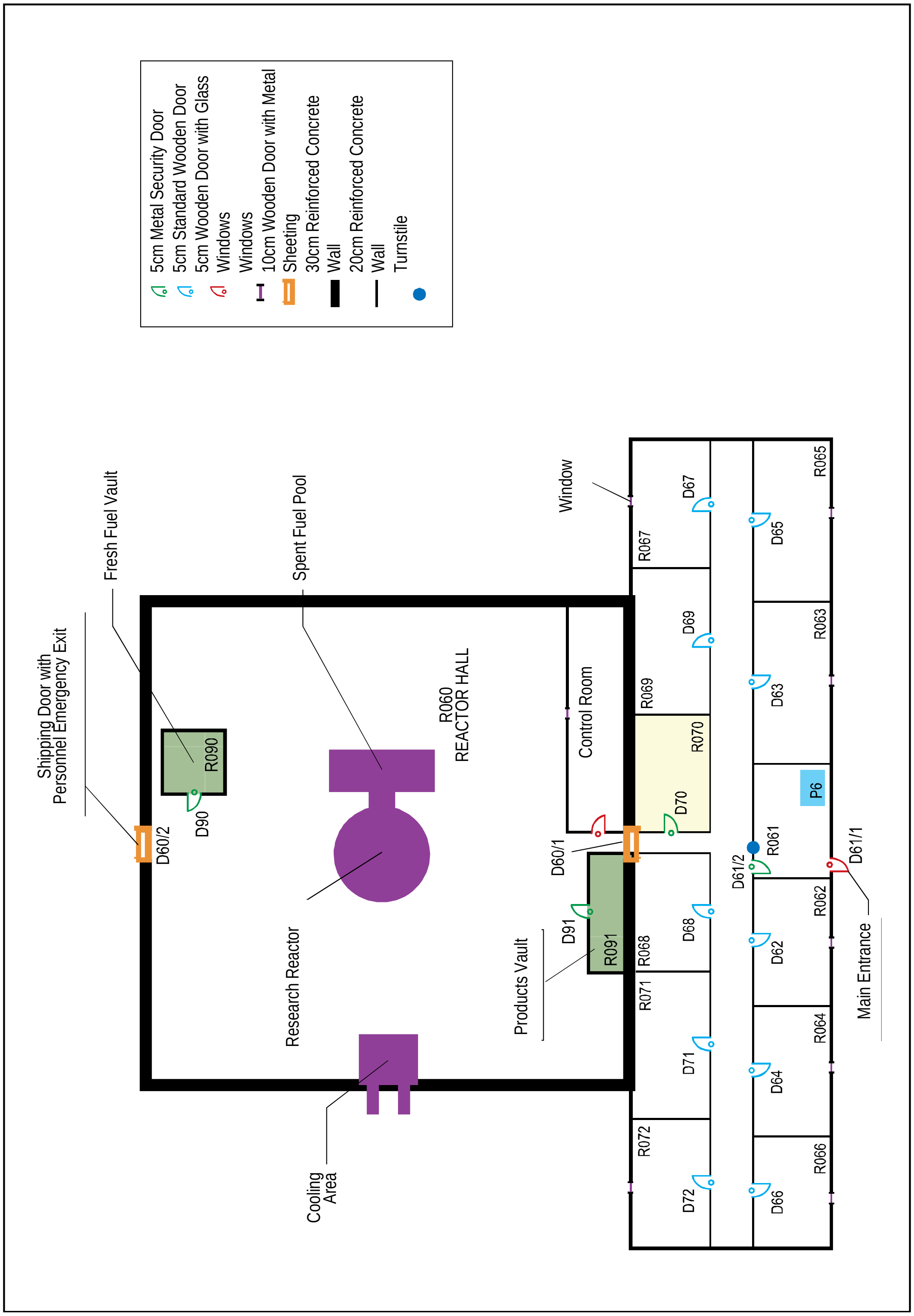
Entry Procedures

1. The CAS operator provides vehicle information to the guard.
2. Under direction from the CAS, a guard unlocks and manually opens the gate.
3. The vehicle drivers slow as they approach the gate.
4. The guard observes the approach of the vehicle for type, speed and suspicious actions. The vehicles must match the description from the CAS.
5. Under the direction and observation of the guard, the driver proceeds through the gate to the PTR building.
6. The guard shuts and locks the gate and remains at the gate for vehicle exit.

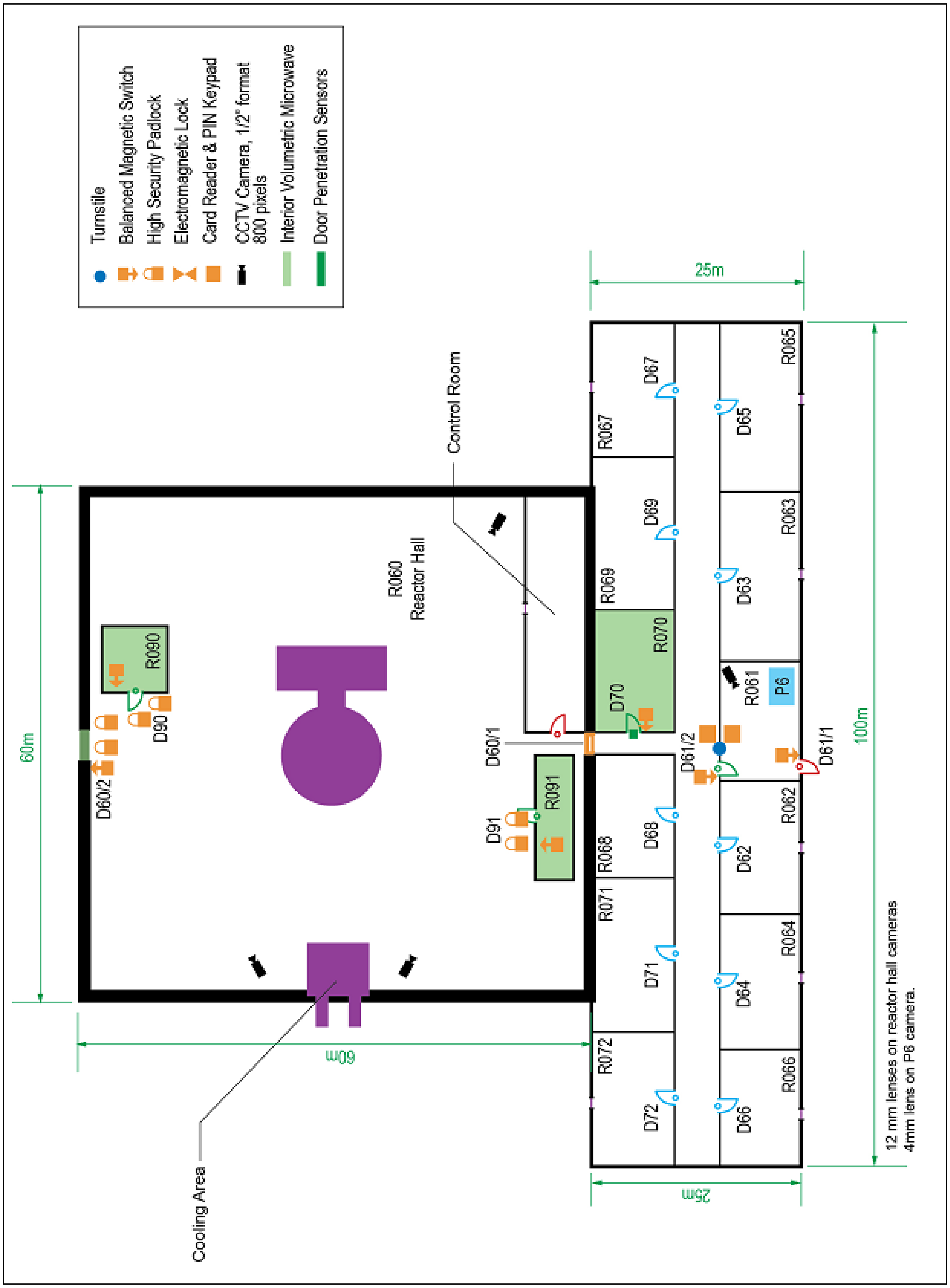
Exit Procedures

1. The CAS operator provides vehicle information to the guard.
2. Under direction from the CAS, a guard unlocks and manually opens the gate.
3. The guard observes the approach of the vehicle for type, speed and suspicious actions. The vehicles must match the description from the CAS.
4. Under the direction and observation of the guard, the driver exits through the gate.
5. The guard shuts and locks the gate.

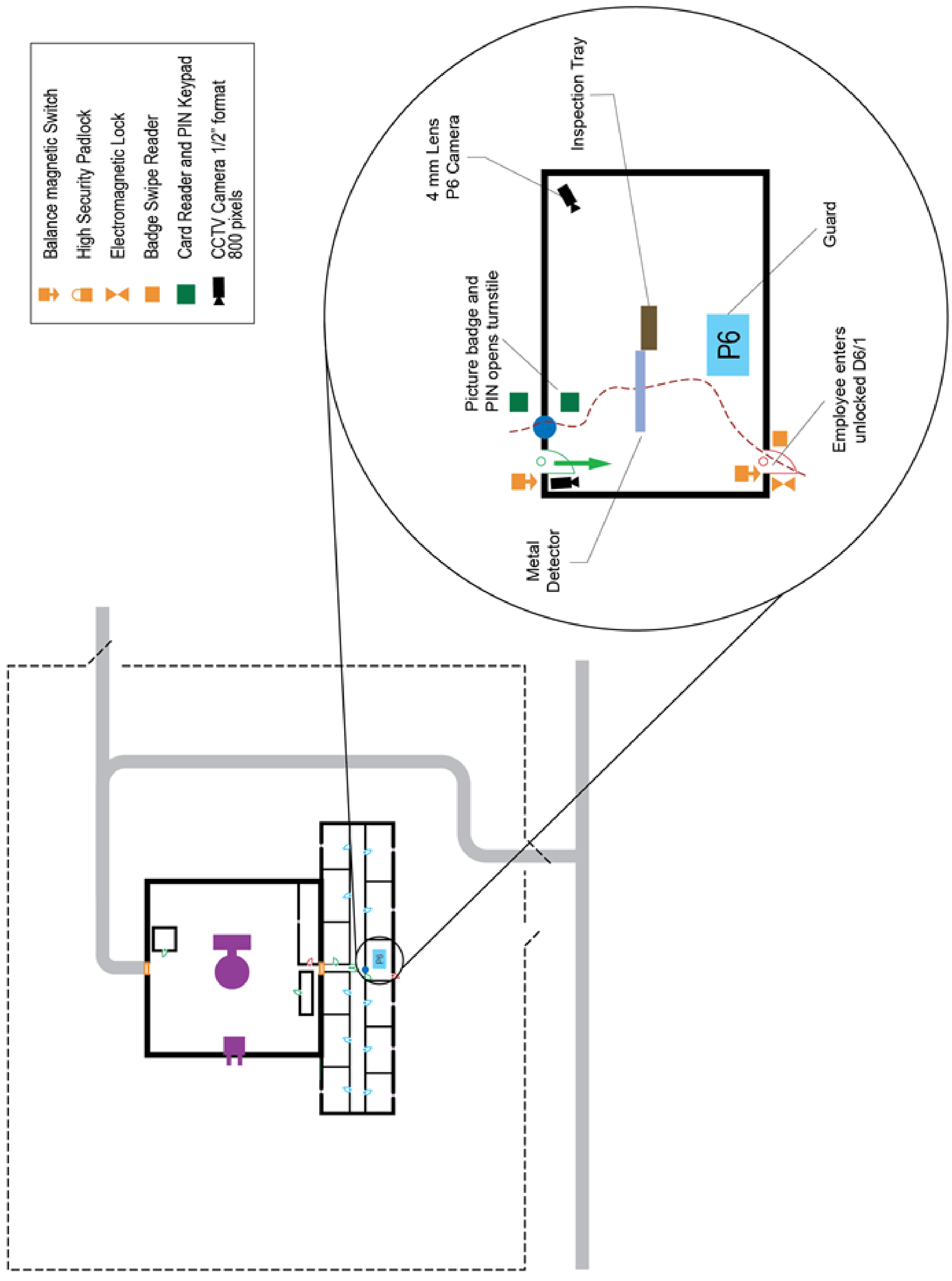
PTR Research Reactor – Building Floor Plan



PTR Interior Physical Protection Elements



PTR Access Control Plan



Personnel

LNRI/PTR On-site Staffing Table			
Position (Number)	**Routine Access**	**Routine Authority/ Responsibility**	**Knowledge**
LNRI Plant Manager (1)	Protected Area, All Inner Areas (usually escorted)	Overall direction. Not authorized to direct detailed facility operations.	General knowledge of plant operations, lacks detailed understanding of facility
Shift Supervisor (1)	Protected Area, All Inner Areas	Detailed direction of all facility activities. Approves all work orders.	Extensive, detailed knowledge about all aspects of facility design, layout, and operation.
Reactor Operators (2)	Protected Area, All Inner Areas	Detailed direction of all reactor operations.	Extensive, detailed knowledge about all aspects of reactor design, layout, and operation.
Operations Support (3)	Protected Area, All Inner Areas	Perform specific operations tasks under direction of the reactor operator and shift supervisor	Specialized knowledge related to their duties. Narrow knowledge of complete facility systems.
Maintenance Manager (1)	Protected Area, All Inner Areas (usually escorted)	Overall direction to maintenance personnel.	General knowledge of plant operations.
Electrical Maintenance (2)	Protected Area, All Inner Areas as work orders specify.	Perform activities on specific systems pursuant to work orders and the plan of the day[i]	Specialized knowledge related to their duties. Narrow knowledge of complete facility systems.
Mechanical Maintenance (2)	Protected Area, All Inner Areas as work orders specify.	Perform activities on specific systems pursuant to work orders and the plan of the day	Specialized knowledge related to their duties. Narrow knowledge of complete facility systems.

LNRI/PTR On-site Staffing Table

Position (Number)	Routine Access	Routine Authority/ Responsibility	Knowledge
Administrative support (4)	Only to the outer office complex. Occasional access to other areas requires escort.	Administrative support	No working knowledge of facility systems.
Health Physics Technicians (2)	Protected Area, all Inner Areas and occasional escorted access to Storage Areas.	Monitor radiological conditions. Not permitted to work on plant equipment	Specialized knowledge related to their duties. Narrow knowledge of facility systems.
Janitorial Staff (2)	Outer office area, Protected Area, and Specific Inner Areas dependent on work assignment.	Cleaning and housekeeping.	No knowledge of plant systems or security measures.
Material Balance Area Custodians (2) ***ALICE***	Protected Area, Inner Areas and Storage Areas	Direct nuclear material inventories, authorize transfers, authorize storage access	Knowledgeable of nuclear material status and inventory procedures. No knowledge of facility systems.
Nuclear Material Technicians (2)	Protected Area, Inner Areas and Storage Areas	Perform nuclear material operations and inventories at the direction of MBA custodians.	Knowledgeable of nuclear material status and inventory procedures. No knowledge of facility systems.
Nuclear Material Accountability Technicians (2)	Escorted access to Protected Area, Inner Areas and Storage Areas	Maintain paper accountability system and generate required nuclear material status, transfer, and inventory reports.	Knowledgeable of nuclear material status and inventory procedures. No knowledge of facility systems.

LNRI/PTR On-site Staffing Table			
Position (Number)	**Routine Access**	**Routine Authority/ Responsibility**	**Knowledge**
Engineering Support (3) ***PAUL***	Only to the outer office complex. Occasional access to other areas requires escort.	Support plant engineering activities.	Specialized knowledge related to their duties.
Design, Mechanical, Electrical, Civil, Chemical and Nuclear Engineers (3)	Protected Area, Inner Areas with escort	Perform design activities and review performance and status of specific systems	Specialized knowledge related to design and performance of specific plant systems. Moderate knowledge of complete facility systems.
Safety Engineers, (2)	Protected Area, Inner Areas with Escort	Analyze safety and impacts of proposed changes, develop / review procedures and procedure revisions, prepare documents for State regulator.	General knowledge of performance and roles of facility systems. No detailed knowledge of operation of complete facility systems.
Security Analyst (1)	Protected Area, Vital Areas with escorts	Perform security analysis activities and review performance and status of specific systems	Specialized knowledge related to design and performance of security systems.
Guard Supervisor	Protected Area, all Inner Areas	Direct activities of security force	No knowledge of facility systems. Knowledgeable about plant security systems and security procedures.

LNRI/PTR On-site Staffing Table			
Position (Number)	**Routine Access**	**Routine Authority/ Responsibility**	**Knowledge**
Alarm Station Operators	Protected Area, Central or Secondary Alarm station.	Monitor alarms and direct response under the direction of the Guard Supervisor	No knowledge of facility systems. Knowledgeable about plant security systems and security operational procedures.
Patrol Guards	Protected Area, all inner Areas	Routine patrol of protected areas and non-radiological vital areas and respond to plant alarms	No knowledge of facility systems. Knowledgeable about plant security systems and security operational procedures.
Post Guards	Protected Area, all inner Areas	Staff access control and other security posts and respond to plant alarms	No knowledge of plant safety / operational systems or plant response to abnormal conditions. Knowledgeable about security operational procedures.

Non-employee Access to LNRI/PTR Table			
Type	**Routine Access**	**Routine Authority / Responsibility**	**Knowledge**
Vendors	Only to the outer PTR office complex. Occasional access to other areas requires escort.	No authority over plant employees.	No knowledge of plant systems, plant response to abnormal conditions, or security measures.
State Safety/security Inspectors	Protected Area and Inner Areas. Employee escort required for all access.	No direct authority over plant employees however suggestions are given great weight.	General knowledge of performance and roles of facility systems.

[i] The plan of the day establishes the maintenance tasks to be performed each day and the systems to be removed from service for maintenance. The shift supervisor or his designee is required to be informed and provide authorization before a system is taken out of service for maintenance.