SAND2015-5497C

Exceptional service in the national interest

Sandia National Laboratories

Photos placed in horizontal position with even amount of white space between photos and header

Approach for Design and Implementation of Protection Measures for the Insider Threat

Carol Scharmer – Sandia National Laboratories

July 14, 2015

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

Contents

Sandia National Laboratories

Security Plan

Sandia National Laboratories

- Basis for licensing
- Based on defined threat
- Based on identified targets
- Based on analysis
- Site specific
- Describes measures to meet Physical Protection requirements
  - Includes Insider Mitigation Programme

Insider Mitigation Plan – How

Sandia National Laboratories

Principles

Policies

Procedures

Insider Mitigation Plan – How

Sandia National Laboratories

Principles

Based on Regulations, define protection strategy

Principles – Insider Threat Examples

Sandia National Laboratories

- *Authorizing access will be strictly controlled.*
- *Trustworthiness determinations and behavioral observation programs will be implemented using a graded approach, where the most rigor is applied to personnel with access to nuclear material, vital areas and sensitive information.*
- *Insider threat mitigation will be an integral part of planning and analysis at the facility level, when designing and implementing protection systems*

Insider Mitigation Plan – How

Sandia National Laboratories

Policies

Rules that implement Principles

Insider Mitigation Plan – How

Sandia National Laboratories

Policy development – Design Process

Defined or derived

Evolve or mature

Policies – Insider Threat Examples

Sandia National Laboratories

- Identity verification for entrance into the Protected Areas will include finger vein biometric verification.
- Only the minimum number of individuals shall be granted authorized access to any designated security area or system.
- No individual shall be granted singular access to nuclear material or critical systems.
- Continuous surveillance will be implemented when personnel require direct access to Category I nuclear material or critical systems in order to perform assigned job duties.

Insider Mitigation Plan – How

Sandia National Laboratories

Procedures

How the rules are implemented

Procedures, continued

Sandia National Laboratories

Administrative Procedures

Procedures, continued

Sandia National Laboratories

Technical Procedures

Procedures, continued

Sandia National Laboratories

Procedures for all situations

Procedures for all situations

Sandia National Laboratories

Normal – situations that have been reviewed

Procedures for all situations

Sandia National Laboratories

Off-normal or Exceptions – for situations that have been reviewed

Procedures for all situations

Sandia National Laboratories

New or Special – situations not previously reviewed

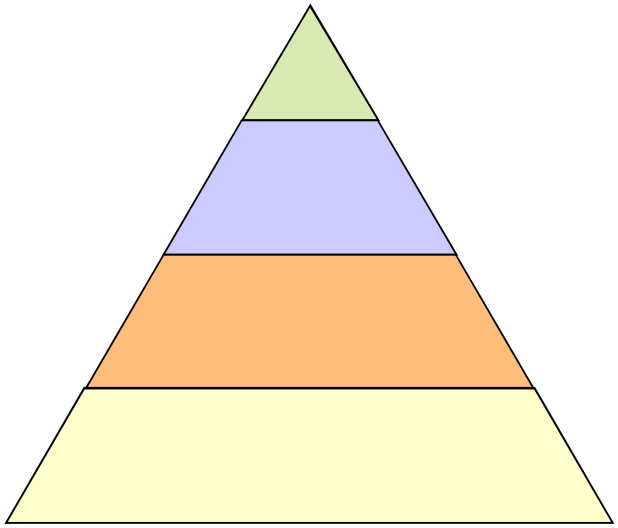
Procedures for all situations

Sandia National Laboratories

Incident – safety or security

Framework

- Principles – regulations
- Policies – rules
- Procedures - implementation



Approach

- Recognize the principles – regulations
- Establish policies – rules
- Establish and document procedures

Example – Required Result

Sandia National Laboratories

Printing and issuing a credential (badge) to an individual

Example – Requires

Access that is

Example – Questions

Where:

Does access need to be controlled?

Example – Questions

Sandia National Laboratories

Who:

Authority to Authorize?

Determines this authority?

Example – Questions

Sandia National Laboratories

What:

Rules to determine access?
Rules to limit authorized access?

Example – Questions

Sandia National Laboratories

When:

When (time of day) is access to each area allowed?

Example – Questions

Sandia National Laboratories

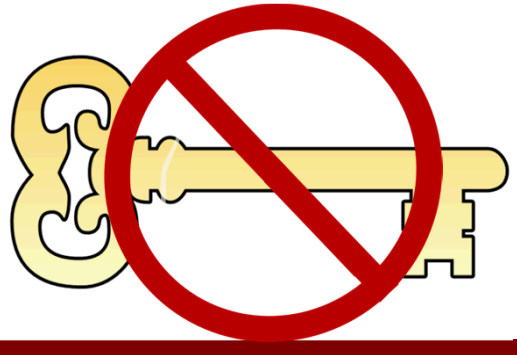
How:

Trustworthiness determined?

Authorized access maintained?

Key control?

Access is terminated?



Example – Principles

- Authorization for access will be strictly controlled.
- Trustworthiness determinations and behavioral observation programs will be implemented using a graded approach, where the most rigor is applied to personnel with access to nuclear material, vital areas and sensitive information.

Example – Policies

- Compartmentalization shall be implemented where feasible.
  - Review of all operational safeguards and security processes shall be reviewed and compartmentalization criteria determined and implemented
  - Compartmentalization criteria should consider individuals with designated authority or specific knowledge.
- Employees working in vital areas or on critical equipment must be vetted and must be in a Behavioral observation program prior to being granted access to the area or equipment.
- Separation of duties shall be applied to job duties in order to limit access to critical equipment and to meet the compartmentalization policy.

Example – Procedures

- Processes for hiring and onboarding, including pre-employment identity and reference checks.
- Process for hiring manager to request employee be issued a badge, including area access requirement/justification.
- Processes to determine need for and enrollment into trustworthiness program
- Review and approval process for access authorization including designation of the individuals with designated approval authority for designated security areas.
  - Includes ensuring authorized access meets rules for compartmentalization and separation of duties

Example – Procedures, continued

- Process for security of personal and sensitive information.
- Process for an employee to receive badge and enroll a personal identification number and biometrics into entry control system.
- Process for removing access when not required and periodic review of required access, including trustworthiness

Example - Electricians

- Hired to perform testing, routine and unscheduled maintenance and to complete minor installations and modifications for electrical systems at a facility.
- Specialized training required to work on control systems, fire alarm system and the security alarm system
- Requirement for 24/7 onsite response to security alarm system outages
- Compartmentalization of systems – location of components and access to the components
  - Emergency Power
  - Reactor Control Systems
  - Communication Network
  - Security system components

Example – Electrician Duties

Sandia National Laboratories

Hypothetical Facility

			Protected Area				Building 1							
Employee	**General Job Duties**	**HRP ? / HRP status**	**Pedestrian Entrance Day / Night**		**Vehicle Entrance Day / Night**		**Main Entrance Day / Night**		**Room 10 (E-power Control Equip) Day / Night**		**Vault 20 (TPR Code Required) Day / Night**		**Room 30 (Reactor Control Room) Day / Night**	
Sammy Smith	LAA Normal Power	No												
Jessie Jones	PA/VA Normal Power	No												
Orville Ortiz	Reactor control systems Maintenance	Yes / In process												
Cassie Clawson	Security Alarms Maintenance	No												
Vladimir Vigil	Security Alarms Maintenance	Yes / Current												
Paddy Perez	Security Alarms Testing	Yes / Current												
Francesca Gao	Emergency Power Systems	Yes / Current												

Example – Authorized Access

Sandia National Laboratories

Hypothetical Facility

			Protected Area				Building 1							
Employee	**General Job Duties**	**HRP ? / HRP status**	**Pedestrian Entrance Day / Night**		**Vehicle Entrance Day / Night**		**Main Entrance Day / Night**		**Room 10 (E-power Control Equip) Day / Night**		**Vault 20 (TPR Code Required) Day / Night**		**Room 30 (Reactor Control Room) Day / Night**	
Sammy Smith	LAA normal power	No	No	No	No	No	No	No	No	No	No	No	No	No
Jessie Jones	PA/VA normal power	No	Yes	Yes	Yes	No	Yes	Yes	No	No	No	No	No	No
Orville Ortiz	Reactor control systems maintenance	Yes / In process	Yes	Yes	Yes	No	Yes	Yes	No	No	No	No	No	No
Cassie Clawson	Security alarms maintenance	Yes/Current	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	No	No
Vladimir Vigil	Security alarms maintenance	Yes / Current	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	No	No
Paddy Perez	Security alarms testing	Yes / Current	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	No	No
Francesca Gao	Emergency power systems	Yes / Current	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	No	No

Note: Authorized means Unescorted Access.

Example – Authorized Access

Sandia National Laboratories

Hypothetical Facility

			Protected Area				Building 1							
Employee	**General Job Duties**	**HRP ? / HRP status**	**Pedestrian Entrance Day / Night**		**Vehicle Entrance Day / Night**		**Main Entrance Day / Night**		**Room 10 (E-power Control Equip) Day / Night**		**Vault 20 (TPR Code Required) Day / Night**		**Room 30 (Reactor Control Room) Day / Night**	
Sammy Smith	LAA normal power	No	No	No	No	No	No	No	No	No	No	No	No	No
Jessie Jones	PA/VA normal power	No	Yes	Yes	Yes	No	Yes	Yes	No	No	No	No	No	No
Orville Ortiz	Reactor control systems maintenance	Yes / In process	Yes	Yes	Yes	No	Yes	Yes	No	No	No	No	No	No
Cassie Clawson	Security alarms maintenance	Yes/Current	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	No	No
Vladimir Vigil	Security alarms maintenance	Yes / Current	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	No	No
Paddy Perez	Security alarms testing	Yes / Current	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	No	No
Francesca Gao	Emergency power systems	Yes / Current	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	No	No

Note: Authorized means Unescorted Access.

Example – Authorized Access

Sandia National Laboratories

Hypothetical Facility

			Protected Area				Building 1							
Employee	**General Job Duties**	**HRP ? / HRP status**	**Pedestrian Entrance Day / Night**		**Vehicle Entrance Day / Night**		**Main Entrance Day / Night**		**Room 10 (E-power Control Equip) Day / Night**		**Vault 20 (TPR Code Required) Day / Night**		**Room 30 (Reactor Control Room) Day / Night**	
Sammy Smith	LAA normal power	No	No	No	No	No	No	No	No	No	No	No	No	No
Jessie Jones	PA/VA normal power	No	Yes	Yes	Yes	No	Yes	Yes	No	No	No	No	No	No
Orville Ortiz	Reactor control systems maintenance	Yes / In process	Yes	Yes	Yes	No	Yes	Yes	No	No	No	No	No	No
Cassie Clawson	Security alarms maintenance	Yes/Current	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	No	No
Vladimir Vigil	Security alarms maintenance	Yes / Current	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	No	No
Paddy Perez	Security alarms testing	Yes / Current	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	No	No
Francesca Gao	Emergency power systems	Yes / Current	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	No	No

Note: Authorized means Unescorted Access.

Example – Authorized Access

Sandia National Laboratories

Hypothetical Facility

			Protected Area				Building 1							
Employee	**General Job Duties**	**HRP ? / HRP status**	**Pedestrian Entrance Day / Night**		**Vehicle Entrance Day / Night**		**Main Entrance Day / Night**		**Room 10 (E-power Control Equip) Day / Night**		**Vault 20 (TPR Code Required) Day / Night**		**Room 30 (Reactor Control Room) Day / Night**	
Sammy Smith	LAA normal power	No	No	No	No	No	No	No	No	No	No	No	No	No
Jessie Jones	PA/VA normal power	No	Yes	Yes	Yes	No	Yes	Yes	No	No	No	No	No	No
Orville Ortiz	Reactor control systems maintenance	Yes / In process	Yes	Yes	Yes	No	Yes	Yes	No	No	No	No	No	No
Cassie Clawson	Security alarms maintenance	Yes/Current	Yes	Yes	Yes	No	Yes	Yes	No	No	No	No	No	No
Vladimir Vigil	Security alarms maintenance	Yes / Current	Yes	Yes	Yes	No	Yes	Yes	No	No	No	No	No	No
Paddy Perez	Security alarms testing	Yes / Current	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	No	No
Francesca Gao	Emergency power systems	Yes / Current	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	No	No

Note: Authorized means Unescorted Access.

Evaluation

If the insider mitigation program is not effectively designed and implemented:

Anyone, regardless of job description or access level, could be or become an insider adversary.

Evaluation – Two Parts

1. Evaluation of the established principles, policies and procedures to requirements
2. Evaluation of the implementation of the procedures to intended design.

Evaluation – Using this Approach

- Advantage 1
  - Measures evaluated prior to implementation
    - The level of detection identified as part of design.

Evaluation – Using this Approach

- Advantage 2
  - Allows design to be based on insider scenarios – NSS13 recommendation

Evaluation – Using this Approach

Sandia National Laboratories

- Advantage 3
  - Access Authorization based on individual job duties, not job description or organization
    - Eliminates assumptions about access that are associated with “Grouping”

Conclusion

Sandia National Laboratories

- Insider Mitigation Framework and Approach
  - Recognize the principles – regulations
  - Establish policies – rules
  - Establish and document procedures
- Addresses complexities
- Access authorization –based on assigned job duties not organization title
- Evaluation
  - Evaluate principles, policies and procedures
  - Evaluate implementation to intended design