

**PSEG NUCLEAR SECURITY**

**SY-AA-101-132**

**Revision 11**

**THREAT ASSESSMENT**

---

**REVISION SUMMARY:**

1. Step 4.5.2 was revised to add greater detail to the reference to SY-AA-101-108. This change specifically address the requirements of 10 CFR 73.55 (g)(4) – In response to a site-specific credible threat or other credible information, implement a two-person (line-of-sight) rule for all personnel in vital areas so that no one individual is permitted access to a vital area. (**Order 80099993 – 0930**)
2. As a result of this review, Step 6.1 was changed from “Commitments” to “Regulatory References” to align with the terms and definitions of LS-AA-110, Commitment Management. Step 6.3.6, previously listed as a writer reference, was moved to Step 6.1.1 and reference to 10 CFR 73.55 (g)(4) was added at Step 6.1.2.

---

**IMPLEMENTATION REQUIREMENTS**

None

## THREAT ASSESSMENT

### TABLE OF CONTENT

<u>SECTION TITLE</u>	<u>PAGE</u>
1. Purpose.....	3
2. TERMS AND DEFINITIONS.....	3
3. RESPONSIBILITIES.....	4
4. MAIN BODY .....	4
4.1. General Information .....	4
4.2. Discovery or Receipt of a threat.....	5
4.3. Investigation.....	6
4.4. Threat Disposition .....	6
4.5. Follow-up Actions.....	7
5. DOCUMENTATION.....	8
6. REFERENCES.....	8
7. ATTACHMENTS.....	9
<b><u>ATTACHMENTS</u></b>	
Attachment 1, Threat Probability and Risk Logic.....	10
Attachment 2, Identification, Assessment and Handling of Potential Security Threats .....	12

## **THREAT ASSESSMENT**

### 1. **PURPOSE**

- 1.1. This procedure sets forth the model to be used as a tool to consider, analyze, and respond to various levels of threats specifically focused toward Salem /Hope Creek Generating Station.
- 1.2. This procedure delineates the responsibilities of the Nuclear Security Director, Security Operations Manager, and the Shift Manager.

### 2. **TERMS AND DEFINITIONS**

- 2.1. **Threat** – an expression of intent to do harm or act out violently against someone or something. A threat can be spoken, written, symbolic, or observed.
  - 2.1.1. **Non-Credible Threat** - a threat which poses a minimal or **no** risk to the safe operation of the facility or to personal and public safety.
  - 2.1.2. **Credible / Possible Threat** - a threat which poses some risk to the safe operation of the facility or to personal and public safety.
  - 2.1.3. **Credible / Actual Threat** - a threat which poses a likely and serious danger to the safe operation of the facility or to personal and public safety.
- 2.2. **Threat Assessment** – an evaluation of a threat, based on physical evidence, observation, the receipt of information however obtained, and its interpretation.
- 2.3. **Direct Information** - identifies a specific act against specific target(s) and is delivered in a straightforward and explicit manner (usually with precise details).
- 2.4. **Indirect Information** - tends to be vague, unclear, and ambiguous. The plan, the intended target(s), motivation, and other aspects tend to be masked or unknown.
- 2.5. **Veiled Information** - strongly implies, but does **not** explicitly threaten an act of violence against target(s); usually a verbal or written hint that "something" will happen.
- 2.6. **Conditional Information** - is often used for extortion and warns of a violent act that will occur unless certain terms or conditions are met.
- 2.7. Cyber-Security Threats related to electrical rotating equipment.
  - The vulnerability that pertains to Digital Protection Control Devices (DPCD) such as protective relays, programmable logic controllers, bay controllers, and other devices that can control breaker closure operations has been mitigated both on-site and off-site in accordance with PSEG's response to NRC letter "Control Systems Vulnerability," dated June 22, 2007.
  - Because these types of threat have been mitigated, **no** additional Nuclear Power Plant Operator actions are required.

### 3. **RESPONSIBILITIES**

#### 3.1. Security Operations Manager

3.1.1. Security Operations Manager and/or designated alternates shall conduct and disposition threat assessment while notifying and working in coordination with appropriate Station personnel.

3.1.2. Security Operations Manager and/or designated alternates shall conduct threat assessment in coordination with applicable Federal, State, and Local Law Enforcement Agencies, when necessary.

#### 3.2. Shift      Manager

3.2.1. Shift      Manager or designated alternate shall assist Security with any ongoing threat assessment. Responsible for contacting NRC Operations Center when applicable.

### 4. **MAIN BODY**

#### 4.1. General     Information

4.1.1. Examples    of possible threats:

- Attack threat (against facility)
- Attack threat (against personnel)
- Vehicular bomb threat
- Water borne threat
- Bomb    threat
- Chemical / biological threat

4.1.2. **ENSURE** every threat is taken seriously until analysis and/or investigation determines threat is **non**-credible, of limited impact, or has been resolved.

4.1.3. **NOTIFY** Security Operations Manager and Shift Manager of the potential threat and that a threat assessment is being performed.

NOTE: All threats are **not** equal in the level of seriousness.

4.1.4. **CONDUCT** threat assessment in a timely manner to assure appropriate classification, disposition and response.

4.1.5. **ENSURE** an effective threat assessment considers all of the information (symptoms) to evaluate threat (similar to how a doctor would approach a medical diagnosis).

NOTE: Assessment must be based on the collective analysis of all factors relating to the threat. Do **not** use only certain details of the threat to drive the outcome.

1. **EVALUATE** all available information of threat.

4.1.6. **MAINTAIN** all materials, documents, or messages relating to a threat.

NOTE: Whenever threat information is received directly via a telephone message, attempt, if possible, to validate the reliability of the source providing the information (i.e., contact the organization for which the caller asserted affiliation). Response actions should **not** be delayed—they should be performed in parallel with the validation.

4.2. Discovery or Receipt of a threat

4.2.1. **If** a threat has been received from NRC and is classified as credible by them, **then** do **not** conduct an additional threat assessment:

1. **ENSURE** the following notifications are made:
  - **NOTIFY** Shift Manager
  - Shift Manager shall **CONTACT** NRC Operations Center.
2. **PROCEED** to section 4.5.

4.2.2. **If** threat has been received from one of the following, **then CONTACT** NRC to assist in validating threat:

- Department of Homeland Security (DHS)
  - Federal Bureau of Investigation (FBI)
  - Federal Aviation Administration (FAA)
  - North American Aerospace Defense Command (NORAD)
1. **If** NRC validates the information as credible, **then** do **not** conduct additional threat assessment.
    - A. **ENSURE** the following notifications are made:
      - **NOTIFY** Shift Manager.
      - Shift Manager shall **CONTACT** NRC Operations Center.
    - B. **PROCEED** to section 4.5.
  2. **If** NRC does **not** validate the information as credible, **then CONDUCT** a threat assessment.
    - **PROCEED** to section 4.3.

4.2.3. **If** threat is received from a source other than NRC, FBI, FAA, DHS, or NORAD, **then** Security shall **INITIATE** threat assessment process upon discovery and/or receipt of a potential threat.

1. **NOTIFY** Security Operations Manager or Designee.
2. **NOTIFY** Shift Manager.
3. **CONTACT** NRC, via Emergency Notification System (ENS) phone **and REQUEST** assistance in verifying credibility of threat.
4. **NOTIFY** Nuclear Security Director.

### 4.3. Investigation

NOTE: Specific detail, plans, or preparation usually suggest a higher risk that the threat will occur--whereas a lack of detail, plans or preparation suggest a lower risk that the threat may occur.

- 4.3.1. **GATHER and DOCUMENT** all information, details, and evidence regarding threat.
1. Specific and plausible details are critical factors in evaluating threat.
  2. Details can include, but are **not** limited to:
    - A. Source of the threat.
      - Who made the threat?
      - To who was the threat made?
      - How was the threat communicated?
    - B. Weapons, explosives, other contraband, or suspicious material.
    - C. Impact of threat to equipment or personnel.
      - What will happen or what will be the result if the threat is carried out?
    - D. Reason(s) or motivation for making threat.
    - E. Means or method proposed to carry out threat.
    - F. Date, time, and location threatened act is supposed to occur.
    - G. Information regarding plans or preparations for carrying out threat.
      - Where did, or will it happen?
    - H. Indication or information regarding similar threats.
      - **CONSIDER** recent, known, or publicized situations or events that have been carried out either inside or outside of nuclear power industry.

### 4.4. Threat Disposition

- 4.4.1. **DISPOSITION** as **non-credible**, **credible/possible**, or **credible/actual** (refer to Attachment 1, Threat Probability and Risk Logic for additional information).
1. **NON-CREDIBLE THREAT** - a threat which poses minimal or **no** risk to safe operation of facility or to personal and public safety.
    - Threat is vague and indirect.
    - Information is inconsistent, implausible, or lacks sufficient details.
    - There may be a general indication of a possible time and location (but **no** exact details).

- Threat lacks realism based on comparison to other events inside or outside the nuclear industry.
  - There is **no** strong indication that the preparation to carry out the threat has been taken.
2. **CREDIBLE / POSSIBLE THREAT** - threat which could pose some risk to safe operation of the facility or to personal and public safety.
- Threat is direct and specific.
  - Threat suggests that definite steps have been taken toward carrying out threat.
  - Threat may compare closely to other events inside or outside of nuclear industry.
  - Evidence substantiating threat may have been discovered.
  - NRC or DHS (Department of Homeland Security) has confirmed a valid threat regarding cyber-security issues.
3. **CREDIBLE / ACTUAL THREAT** - a threat which poses a likely and serious danger to safe operation of the facility or to personal and public safety.
- Evidence clearly substantiating threat has been discovered.
  - Threat has occurred, is approaching, or is impending within a short time period.
  - NRC or DHS (Department of Homeland Security) has confirmed a valid threat regarding cyber-security issues.

#### 4.5. Follow-up Actions

- 4.5.1. **If** credible threat information is received from the NRC **or** threat information received from the FBI, FAA, DHS, or NORAD has been validated as credible by the NRC **or** if information is received from any source and all of the conditions (listed below) are met, **then CLASSIFY** threat as **CREDIBLE / ACTUAL THREAT**.
- Threat is focused at Salem/Hope Creek.
  - Threat is considered credible.
  - Threat is specific.
  - Threat is impending [ $< 2$  hours].
1. **ENSURE** the following actions are taken:
- **IMPLEMENT** Emergency Plan.
  - **IMPLEMENT** Operation's Special Event / Abnormal procedures.
  - **REFER** to Attachment 2, Identification Assessment and Handling of Potential Security Threat, for further actions and notifications.

- 4.5.2. If conditions listed in Section 4.5.1 have **not** been met, but threat has still been dispositioned as **CREDIBLE / POSSIBLE**, then Shift Manager to perform the following:
- **IMPLEMENT** OP-AA-106-101-1002.
  - **NOTIFY** PSEG Senior Management.
  - **IMPLEMENT** SY-AA-101-108, Section for Existence of Specific, Credible Insider Threat (Implementing a two person (line-of-sight) rule in vital areas).
  - **REFER** to Attachment 2, Identification Assessment and Handling of Potential Security Threat, for further actions and notifications.
- 4.5.3. In all cases, **IMPLEMENT** appropriate actions in accordance with:
1. Station Security Plan
  2. Security Contingency procedures
  3. Safeguards Event Report
- 4.5.4. **CONTACT** the following off-site agencies as appropriate in accordance with phone list in SY-AA-101-121-1001, Security Communication Network:
1. Local Law Enforcement Agency
  2. State Police
  3. Regional Operations & Intelligence Center (ROIC)
  4. Federal Bureau of Investigation
  5. Nuclear Regulatory Commission
- 4.5.5. **INITIATE** notification of appropriate personnel (refer to Attachment 2, Identification, Assessment and Handling of Potential Security Threats).
5. **DOCUMENTATION**
- 5.1. As data is collected throughout threat assessment process, it is important that all documents be maintained in an organized and controlled manner at the site.
- 5.2. All follow-up actions should be documented and formally tracked.
6. **REFERENCES**
- 6.1. Regulatory References
- 6.1.1. Item B.3.c. of NRC Order for Interim Safeguards and Security Measures dated February 25, 2002 (Attachment 2)
- 6.1.2. 10 CFR 73.55 (g)(4) – In response to a site-specific credible threat or other credible information, implement a two-person (line-of-sight) rule for all personnel in vital areas so that no one individual is permitted access to a vital area.

6.2. User References

- 6.2.1. SY-AA-101-108, Response to Suspicious Activity and Events Maliciously Directed at Plant or Security
- 6.2.2. SY-AA-101-109, Response to Contingency Events
- 6.2.3. SY-AA-101-111, Threat Advisory Protective Measures System
- 6.2.4. SY-AA-101-121- 1001, Security Communication Network
- 6.2.5. OP-AA-106-101, Significant Event Reporting
- 6.2.6. OP-AA-106 -101-1002, PSEG Nuclear Issues Management
- 6.2.7. Emergency Plan
- 6.2.8. Emergency Plan Annexes (to include Emergency Activation Levels)
- 6.2.9. SY-AA-1002, Safeguards Event Report (SER)
- 6.2.10. Letter from U.S. NRC to Wm. Levis, "Control Systems Vulnerability," dated June 22, 2007

6.3. Writer's References

- 6.3.1. Fein, R.A., & Vossekuil, B. (1998). Protective Intelligence Threat Assessment Investigations: A Guide for State and Local Law Enforcement Officials.
- 6.3.2. National Center for the Analysis of Violent Crime, FBI Academy (1998). The School Shooter: A Threat Assessment Perspective.
- 6.3.3. Van Zandt & Associates (2001). Guidelines for Threat Assessment Decision Making
- 6.3.4. NRC Order for Interim Safeguards and Security Measures (dated February 25, 2002)
- 6.3.5. Safeguards Advisory for Operating Power Reactors, SA-04-07 (dated June 18, 2004); ***this document is classified as Safeguard Information***

7. **ATTACHMENTS**

- 7.1. Attachment 1, Threat Probability and Risk Logic
- 7.2. Attachment 2, Identification, Assessment and Handling of Potential Security Threats

**ATTACHMENT 1**  
**Threat Probability and Risk Logic**  
**Page 1 of 2**

**THREAT PROBABILITY:**

- **High Probability** - strong belief the threat is both credible and is likely to occur based as threatened
- **Moderate Probability** - threat is deemed possible, but there is **no** indication of actual credibility or time/date of occurrence is vague
- **Low Probability** - **no** information to confirm threat and information and assessment made does **not** support possibility of threat being carried out as threatened

Probability Considerations:

- Use of technical acronyms or jargon or indication the person making threat is technically trained merits close attention.
- The more specific details contained in threat, the more likely threat is to be credible. **[Moderate to High probability]**
- **If** details are vague, less likely threat is to be credible. **[Moderate to Low probability]**
- **If** a written threat is lengthy (1 or more pages) or appears to be have been carefully planned or invokes religious or group affiliation, **then** the threat tends to be credible **[Moderate to High probability]**.
- **If** a written threat is simply a few sentences with vague information, **then** the threat tends to be less credible **[Moderate to Low probability]**.
- **If** technical terms are used (\*For Example, if there is a technical term for threatened device or substance, or for its effects), **then** it is a **[Moderate to High probability]**.  
\*This includes the size of the device, the power, or in the case of chemical or biological agents, any reference to the lethal dose, incubation period, etc.

**ATTACHMENT 1**  
**Threat Probability and Risk Logic**  
**Page 2 of 2**

**RISK LOGIC EXAMPLES**

Situation A: A bomb threat is received from an organization that is claiming responsibility for placing the device. The message indicates the type of bomb, what type of equipment will be destroyed, how the bomb was introduced to the facility, and the time it is intended to explode.

Logic: **Based on this information, the risk logic would indicate a MODERATE probability because this threat contains specific details and suggests that planning and preparation took place. If a search of the area resulted in the discovery of an explosive device, then the probability would escalate to HIGH in accordance with a credible/actual threat.**

---

Situation B: A powdered substance is discovered on the floor of an area of the plant and two employees are concerned that it may be a type of biological threat. The investigation revealed that grinding was being performed in an area adjacent to where the powdered substance was found. It appears that the substance, created by the grinding process, was transferred to the plant by personnel passing through the work area.

Logic: **Based on this information, the risk logic would indicate LOW equivalent to a non-credible threat. This is due to a logical explanation for the presence of the substance, and the lack of detail, motivation, and a substantiated threat.**

**ATTACHMENT 2-Identification, Assessment, and Handling of Potential Security Threats**  
**Page 1 of 1**

