Title of Paper: A Practical Approach to Assessing Nuclear Threats
Author: Roberta S.Warren, U.S. Nuclear Regulatory Commission, USA

Abstract: An important component of assuring adequate protection for Nuclear and Radiological materials is understanding the significance of potential threats. In a regulatory environment, there is a need for a consistent and transparent approach to determining the credibility and seriousness of a potential threat that can be used across the sector. In the United States, the Nuclear Regulatory Commission (NRC) has established a small cadre of experts who are responsible for assessing threats made to the regulated nuclear industry. The Information Assessment Team (IAT) is available through the NRC Operations Center 24/7 and is made up of threat analysts, security specialists and, as needed, reactor, materials and cyber technical experts. This Team can also reach out to law enforcement and intelligence agencies, as well as the licensee personnel involved.

Introduction: In the post 9/11 environment, understanding the significance of threats involving nuclear and radiological facilities and materials is of even greater importance. A threat may impact a particular licensee or class of licensees, or may have broader implications for other types of critical infrastructure. It is therefore imperative that a process be in place to assess threats in a timely and effective manner and that ensures that all appropriate entities are informed, including licensees, law enforcement, intelligence and homeland security agencies.

The NRC's historical experience showed that response to evaluating threats was very inconsistent and dependant on the experience of the recipient of the initial threat information. In some cases, the recipient overreacted to the information, and in other cases, insufficient action was taken regarding the threat. Out of these real-life experiences, the Information Assessment Team (IAT) concept was developed.

The Information Assessment Team: The IAT is the NRC focal point for assessing all reported threats and threat-related information involving NRC licensed facilities, materials and activities. A threat is defined as information – explicit or implied, written or verbal – that a malevolent act may be committed against licensed or certified nuclear facilities, materials or activities. A "threat" is distinct from acts that are in progress or that already occurred. The IAT is responsible for assessing threats or threat-related events, whereas responsibility for responding to safety or security events that have already occurred, including a licensee's decision to implement their emergency plan, rests with the NRC Headquarters Operations Center and the NRC Incident Response Teams at the Headquarters and Regions.

All members of the Team are trained, carry mobile phones and/or pagers and are responsible for responding telephonically to assess threats as quickly as possible, usually returning calls to the Operations Center within minutes. Team members consist of highly experienced threat analysts, physical security specialists, and when necessary, reactor,

material or cyber technical experts. Licensee security managers, law enforcement, intelligence and homeland security agencies can also be brought into the deliberations. In most cases, threats can be resolved during the initial phone call. If the situation warrants further actions, recommendations can be made to NRC management to elevate the response, including responding to the declaration of different emergency levels. Recommendations can also be made to the licensee regarding possible elevations of site security measures. If the threat presents potential implications to other licensees or non-NRC-related interests, additional notifications will also be made. If there is potential media interest, Public Affairs officials can also be notified. Although the IAT focuses on threats, the Team remains on-call during an agency response to assist NRC staff in reviewing events or to react to other incidents for threat-related implications.

Handbook of potential scenarios: In order to facilitate the discussions and guide potential actions, a handbook of potential scenarios and questions to consider during deliberations has been developed. The general categories of scenarios include:

1. Suspected Tampering, Vandalism, Sabotage
2. Suspected or Actual Intrusion (Unauthorized entry)
3. Nuclear Extortion Threat
4. Suspected Theft of Special Nuclear Material (Unlawful Diversion)
5. Bomb Threat
6. Suspected Arson
7. Radiological Dispersal Device (RDD) Threat
8. Radioactive Contamination Threat
9. Non-Specific Threats
10. Computer System or Cyber Threat

For example the factors to consider for "Suspected Tampering, Vandalism, Sabotage includes the following:

1. Upon identification of suspected tampering, vandalism, and/or sabotage, has the licensee contacted local law enforcement-to include their supporting local Federal Bureau of Investigation (FBI) field office (the responsible National-level law enforcement agency)? Also, has the associated area been cordoned off-in as much as physically possible-to protect evidence?
2. Does the reported action prevent a safety system from performing its intended function? What are the consequences of the reported action/activity? Does the target of the reported action and timing clearly demonstrate an intention to cause an interruption of reactor operation, an accident condition, or other unacceptable consequences?
3. Does the reported action prevent a safety system from performing its intended function? What are the consequences of the reported action?
4. Does the reported action by itself render a safety or mitigation system inoperative, or are other system failures required before the safe operation if the plant is at risk? What are those systems and what is their current status?
5. Does the reported action affect special nuclear materials?

6. What is the current operating status of the reactor – has normal operation of the reactor been interrupted? Is the facility in some type of outage?
7. Does the reported action involve more than one structure, system or component? Are they physically separated?
8. Could the reported action be the result of operator and/or maintenance error? Is there any overt evidence, e.g., cut wires or chains, damaged equipment, etc.?
9. Has any threat been communicated that could relate to the reported action?
10. Are there existing, or recent, labor concerns at the facility?
11. What steps has the licensee initiated to assure that no other acts of tampering have occurred or will occur?
12. What is the current status of site security?
13. Has the site initiated an internal investigation?
14. Can operating conditions be changed to mitigate or prevent undue risk?
15. Is there any recent site history of suspected tampering or vandalism? Is there any trend or pattern?
16. Is there media attention?

As demonstrated by the above questions, the initial assessment is used to evaluate the situation from a safety and operational perspective, as well as from a security and investigative perspective. The goal is to understand if there is an immediate threat to the safe operation of the plant and also if there are potential underlying security issues that need to be addressed. Responsibilities for responding to the potential threat belong primarily to the licensee, as well as the responding law enforcement agencies. NRC, as the regulatory authority, has responsibility for ensuring the response by the licensee is adequate to assure the protection of public health and safety.

Another example is the factors considered for a "Bomb Threat:"

1. Has local law enforcement, including the local FBI office, been notified? If so, what is the nature of their response?
2. Has local law enforcement or the FBI provided an initial assessment on the credibility of the threat?
3. What are the circumstances surrounding the reported threat? Who, when and how was the threat received? How was the threat communicated – letter, audio or video recording, email, telephone call, etc.?
4. If the threat was communicated by telephone, did the recipient note all of the threat that can be remembered or was the call recorded? Who has possession of the letter, recording, or email, that contained the threat and is it secure and being treated as evidence? If there is any physical evidence, it should be provided to law enforcement as quickly as possible.
5. Would the threatened action prevent a safety system from performing its intended function? What are the consequences of the reported action? Does the target of the threatened action and timing clearly demonstrate an intention to cause an interruption of reactor operations, an accident condition, or other unacceptable consequences?

6. Would the threatened action prevent a system designed to support a safety system from performing its intended function? What are the consequences of the reported action?
7. What is the current operating status of the reactor? Has normal operation of the reactor been interrupted?
8. Does the threat contain a deadline?
9. Would the threatened action involve more than one structure, system or component? Are they physically or geographically separated?
10. Has the facility received any other threats that could be associated with the current threat?
11. Has any suspicious device or activity been identified recently?
12. What is the current status of site security?
13. Can operating conditions be changed to mitigate or prevent undue risk at the facility?
14. Are there any existing labor concerns at the facility? Has anyone recently had his/her employment terminated for cause?
15. Is there any recent history of suspected tampering or vandalism?
16. Is there any evidence of "insider" involvement?
17. Is there any media attention?

The above are only two examples of the types of questions that have been developed relative to the particular "threat scenario" involved. It is important that threat evaluation guidance be developed prior to the actual need for evaluating a threat occurs as often such situations move very quickly and can be stressful if participants are unprepared.

Database development: A valuable step that the NRC took immediately following the events of 9/11 was the development of a database to record the threats and security events that occurred. The database contains records of all pertinent data concerning the circumstances of the threats or events, as well as the resulting investigation and final resolution. The database, which is password protected and has all privacy-related information removed, is available to licensees and appropriate government agencies with a need-to-know. The data can be searched in a number of ways and is used for development of trend reports which can facilitate security improvements and policy development. The data is also being fed into national-level evaluations of threats against all elements of the critical infrastructure, looking for similarities and possible connections.

Conclusion: The Information Assessment Team approach has proven to be an effective and efficient process to quickly assess the seriousness of threats to the U.S. commercial nuclear sector and ensure appropriate coordination with licensees, law enforcement and other relevant agencies. The concept could be adapted to a country's regulatory, legal and organizational structure. The key element is having a process in place with a small group of threat, technical and security experts being available to quickly respond and develop an initial assessment. Often threats are only viewed as a security or law enforcement issue, but having the ability to also evaluate the safety implications at the same time is critical to ensuring that the public health and safety is adequately protected,

while dealing with the threat or security issues. Working with all of the agencies that would need to be involved in the initial assessment will ensure that all aspects of a threat will be considered and both the safety and the security impacts are considered. This can also enhance the routine sharing of information between the regulatory authority and the law enforcement and security agencies.