History of Suspicious Activity Reporting

Background

Following the events of September 11, 2001, the U.S. Nuclear Regulatory Commission (NRC) issued several security advisories and other guidance related to event reporting. On October 8, 2004, the staff issued Information Advisory Team Assessment (IA)-04-08, "Reporting Suspicious Activity Criteria" (Agencywide Documents Access and Management System (ADAMS) Accession No. ML090570321 (non-publicly available)), requesting various classes of licensee facilities to report suspicious activities to the NRC. IA-04-08 applied to power reactors, decommissioning reactors, non-power reactors (research and test reactors), Category I fuel cycle facilities, gaseous diffusion plants, independent spent fuel storage installations, conversion facilities, and certain large byproduct materials licensees.

On March 19, 2013, the NRC published 10 CFR Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material," in the *Federal Register* (78 FR 17007). Section 37.57(b) requires licensees possessing category 1 or category 2 quantities of radioactive material to report certain suspicious activities at their facilities to the NRC. This superseded the guidance in IA-04-08 for "large byproduct material licensees."

On January 24, 2005, the U.S. Department of Homeland Security (DHS) issued a memo containing guidance developed by DHS and the Federal Bureau of Investigation (FBI) on "[U] Terrorist Threats Reporting Guide for Critical Infrastructure and Owners and Operators" (referred to as the TTRG) (ADAMS Accession No. ML17081A395 (non-publicly available)). The NRC's direction to licensees in implementing the TTRG is found in the "Reporting Guidance" section of the TTRG.

Current Status of Suspicious Activity Reporting

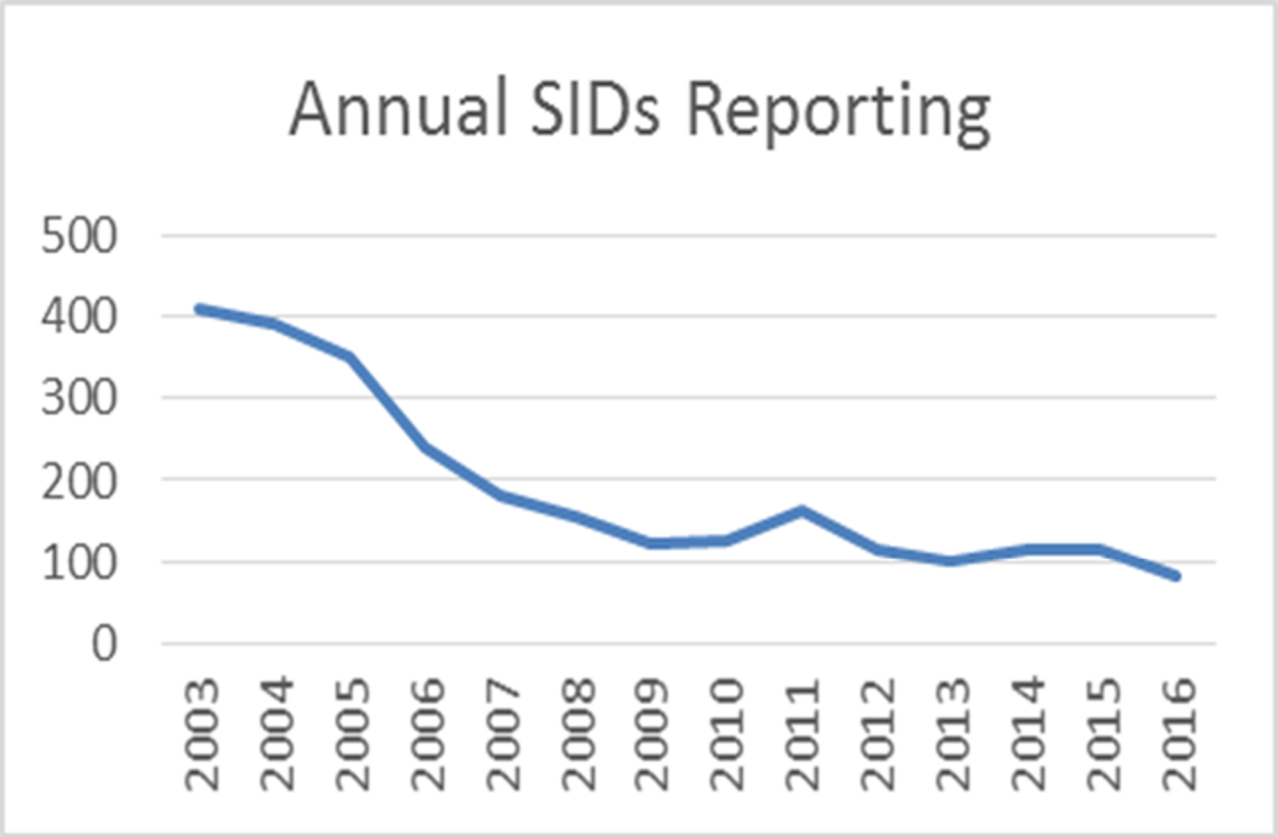
Since voluntary reporting of suspicious activities began after the events of September 11, 2001, the NRC has been tracking the reports submitted to the NRC Headquarters Operations Center using the Security Information Database (SID). The NRC's Intelligence Liaison and Threat Assessment Team (ILTAT) members in Region IV review all of the reports submitted into the SID and then follow up with the appropriate FBI local field office. Other Federal and State agencies, such as the FBI or DHS, routinely query the SID and conduct any necessary follow-up investigations. When licensees first began reporting suspicious activities into the SID in 2004, they submitted approximately 400 reports the first year. In 2016, licensees submitted 77 SID reports. Figure 1 below shows that there was a large decline in the number of SID reports from 2003 to 2007.[1] The staff attributes this decline to more realistic reporting following the initial over-conservatism and heightened sensitivity to potential suspicious activities in the period immediately following the events of September 11, 2001.

As can be seen in Figure 1, from 2009 to 2015, the number of SID reports was relatively consistent (except for 2011). The trends from 2015 and 2016 and the extrapolation of current data for 2017 are of more relevance. The 2014 to 2016 time period shows a yearly decline in the total number of SID reports, with the decline continuing in 2017. Moreover, the staff's analysis of the database from 2014 through 2016 indicates that a number of licensees reported

[1] The NRC issued initial guidance on reporting suspicious activities in October 2001. The current guidance, IA-04-08, was issued in 2004 and superseded the initial guidance to industry. In 2003, the NRC established the Protected Web Server (PWS) to serve as a repository for SID reports that was accessible to both the NRC and licensees. The information in Figure 1 is based upon data from the PWS.

no suspicious activities during these years. The staff cannot discern whether this decline is due to a decrease in suspects contemplating a potential attack against an NRC-regulated facility or due to a decrease in licensee conformance with the voluntary guidance in IA-04-08. However, based on information collected by the intelligence community and consideration of the current threat environment, the staff views the latter rationale more likely than the former.

Figure 1: Annual SIDs Reporting vs. Time



Although the NRC does not participate in investigations conducted by the intelligence community, the NRC's ILTAT identified several recent suspicious activity reports (SARs) that resulted in detailed follow-up investigations by the FBI or State law enforcement agencies. None of these investigations led to criminal prosecutions. However, follow-up visits by FBI or local law enforcement agency (LLEA) personnel may dissuade or potentially disrupt potential attacks. Moreover, ILTAT indicated that, in recent years, the intelligence community has seen an increase in the number of terrorist attacks within the United States These attacks have shifted from complex attacks against critical infrastructure (seen in the events of September 11, 2001) to attacks against softer targets, especially by homegrown violent extremists.

The DHS and FBI continue to view SARs from critical infrastructure owners and operators as key to maintaining situational awareness over these sectors and providing early warning of potential malevolent acts. Despite the increasingly fluid and unpredictable nature of the threat environment, some elements of terrorist tactics, techniques, and procedures remain constant. For example, attack planning and preparation generally proceed through several predictable stages, including intelligence gathering and pre-attack surveillance or reconnaissance. These pre-attack stages, in particular, offer law enforcement and security personnel the greatest

opportunity to identify and disrupt or dissuade acts of terrorism before they occur. To use this information most effectively for disrupting or dissuading potential terrorist attacks, timely reporting of suspicious activities by licensees to both Federal and local law enforcement is of vital importance.

A licensee's timely submission of SARs to the Federal and local law enforcement is an important part of the U.S. government's efforts to disrupt or dissuade malevolent acts against the nation's critical infrastructure. The staff also recognizes that pre-attack surveillance or reconnaissance activities can occur as single instances across multiple sectors, as well as multiple instances across a single sector. Consequently, integration of suspicious activity reporting at a national level, across multiple critical infrastructure sectors, is vital to the effective functioning of these intelligence fusion centers. The staff also notes that DHS continues to invest information technology resources to update its infrastructure for suspicious activity reporting and communication.

Suspicious Activity Reporting in the Draft Final Rule

The draft final rule would incorporate provisions similar to those that had been contained in IA-04-08. The draft final rule requires notification of suspicious activities that take place at nuclear power reactor facilities, Category I strategic special nuclear material (SSNM) facilities, non-power production or utilization facility, and other nuclear spent fuel and high-level radioactive waste facilities, or during the transportation of spent nuclear fuel, high-level radioactive waste, or SSNM. The draft final rule would not apply to Category II or III special nuclear material (SNM) fresh fuel fabrication facilities. However, the draft final rule would apply to Category II or III SNM enrichment facilities, but only with respect to their Restricted Data (RD) materials, technology, and information used in the enrichment process. The draft final rule takes this approach due to the national security non-proliferation concerns associated with RD materials, technology, and information. As previously discussed, industry as evidenced by comments received from the Nuclear Energy Institute, is generally supported of the suspicious activity reporting requirements in the draft final rule.

The draft final rule includes provisions on reporting suspicious activities to local law enforcement, the FBI, the NRC, and the Federal Aviation Administration (FAA) (for suspicious activities involving aircraft). However, in response to concerns identified during the development of the draft final rule, the staff has revised the language to accomplish several objectives:

- Simplify the potential activities to be reported and provide additional time for licensees to complete actions, such as:
    - Licensees would report suspicious activities "as soon as possible, but within 8 hours of the time of discovery."
    - Licensees would be encouraged to use their best judgement and knowledge of their surroundings to promptly assess whether an activity was suspicious.
    - Licensees could take into account knowledge of their surroundings and could gather additional data (e.g., querying local or campus police) to assess whether an activity was suspicious.
- Narrow the classes of facilities and activities appropriate for such reporting;

- Provide additional clarifying examples, both reportable and not reportable, in the new associated Regulatory Guide (RG) 5.87, “Suspicious Activity Reports (U)”;
- Clarify that a licensee’s decision to report is final and does not need to be retracted; and
- Recognize that this information is perishable and best value is obtained by quickly notifying law enforcement (to maximize their likelihood of disrupting or dissuading a terrorist act).

For the new suspicious activity requirement, the staff intends to encourage timely reporting by licensees while minimizing unnecessary reports. The staff does not intend that the requirements be used to evaluate a licensee’s conclusions as to whether an event is suspicious. The draft final rule (Enclosure 1) explains that enforcement action would be limited only to findings for which a licensee does not have a process in place for reporting suspicious activities or for which a licensee has not identified the contact information, for example, the FBI local field office. This clarification enhances the flow and consistency of usable information to law enforcement agencies and the intelligence community.

The staff has segmented this new requirement into a new separate section, 10 CFR 73.1215, “Suspicious activity reports,” and created a new supporting RG 5.87 to increase regulatory clarity.

The draft final rule exempts three Category III SNM licensees from the SAR requirements. These licensees are identified by their docket ID number in the draft final rule under 10 CFR 73.1215(g). They possess their SNM encapsulated in sealed sources that are used for research, development, and testing purposes. The staff recommends this approach given the decreased security risk posed by these licensees since the SNM is contained in sealed sources. The staff has recommended this exemption to reduce the burden on these small licensees while considering the relative radiotoxicity of this SNM, when compared to byproduct material sealed sources which are subject to the similar SAR requirements under 10 CFR 37.57, “Reporting of events.”

Advantages and Disadvantages of Establishing a Reporting Requirement

As mentioned in the Commission paper, to support the Commission’s evaluation of this issue:

(1) The staff has included a detailed discussion of the advantages and disadvantages of suspicious activity reporting, below.

(2) The staff has separated the suspicious activity reporting requirement rule language, regulatory guidance, and other supporting sections in the draft final rule package for the Commission to review and consider independent of the other final enhanced weapons rule requirements.

Advantages of this new requirement:

- Codifies current voluntary efforts by industry;
- Increases regulatory clarity to licensees, ensuring consistent reporting to all elements of the reporting chain (i.e., LLEA, the FBI, the NRC, and the FAA (for suspicious activities involving aircraft)), which increases the potential for disrupting or dissuading potential terrorist attacks;

- Increases consistency of reporting by licensees to the NRC for integration into the threat assessment process, which is one of the NRC's two primary mission essential functions;
- Increases the length of time available to licensees to assess whether a potential activity is suspicious and thus should be reported;
- Provides licensees the opportunity to gather additional information during the assessment process and use their best knowledge of their locale and the local population to reach a conclusion as to whether an activity is suspicious; and
- Increases clarity associated with the new reporting language, new guidance direction and examples, and enforcement guidance (focused on process not events).

Disadvantages of this new requirement:

- Establishes a new reporting requirement and associated burden on licensees;
- Does not decrease any assessment and communication burden for licensees who are currently voluntarily reporting suspicious activities;
- Requires licensees to revise or develop suspicious activity reporting procedures and train key personnel on the new standards;
- Obligates licensees who have chosen to not participate in the current voluntary suspicious activity reporting program to comply with the new provisions in the draft final rule;
- Requires NRC resources to develop inspection and enforcement guidance; and
- Proceeds to rulemaking without attempting to adjust voluntary guidance to address consistency of suspicious activity reporting.