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 suspicious activity and event reporting.[1] 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, Category I fuel cycle facilities, gaseous diffusion plants, independent spent fuel storage installations, conversion facilities, and certain large byproduct materials licensees. While the staff has issued a number of security and threat advisories since 2005, the suspicious activity reporting guidance in IA-04-08 has not been updated since its issuance in 2004.

On January 24, 2005, the U.S. Department of Homeland Security (DHS), in conjunction with the Federal Bureau of Investigation (FBI), issued a document entitled Terrorist Threats to the U.S. Homeland Reporting Guide for Critical Infrastructure and Key Resource Owners and Operators (TTRG) (ADAMS Accession No. ML17081A395 (non-publicly available)). DHS issued the document to leverage the resources of the nation's critical infrastructure partners in recognizing and reporting activities that may be indicative of terrorist-related activity. Accordingly, DHS's TTRG identifies common indicators and patterns that may be associated with terrorist threats and encourages critical infrastructure owners and operators to report relevant indicators and patterns to local law enforcement and homeland security officials. The TTRG further explicitly encourages NRC licensees to continue reporting suspicious activities to the NRC in accordance with IA-04-08.

In response to NRC guidance, licensees began voluntarily reporting suspicious activities to the NRC and local law enforcement after the events of September 11, 2001. Reports were submitted to the NRC Headquarters Operations Center and entered into the Security Information Database (SID). From Calendar Year (CY) 2003 through CY 2005, the annual average number of suspicious activity reports submitted was 419 (See Figure 1 below). Beginning in CY 2006, there was a significant decline in the number of suspicious activity reports submitted to the NRC. For example, in CY 2006, the total number of reports submitted fell to 244 from the CY 2005 total of 446 reports. Similarly, the CY 2007 number of reports fell to 183 and the CY 2008 number of reports fell to 164 (See Figure 1 below). During the period CY 2006 through CY 2008, the number of suspicious activity reports averaged 197. The staff attributes this decline to more realistic reporting following the initial heightened sensitivity to potential suspicious activities in the period immediately following the events of September 11, 2001.

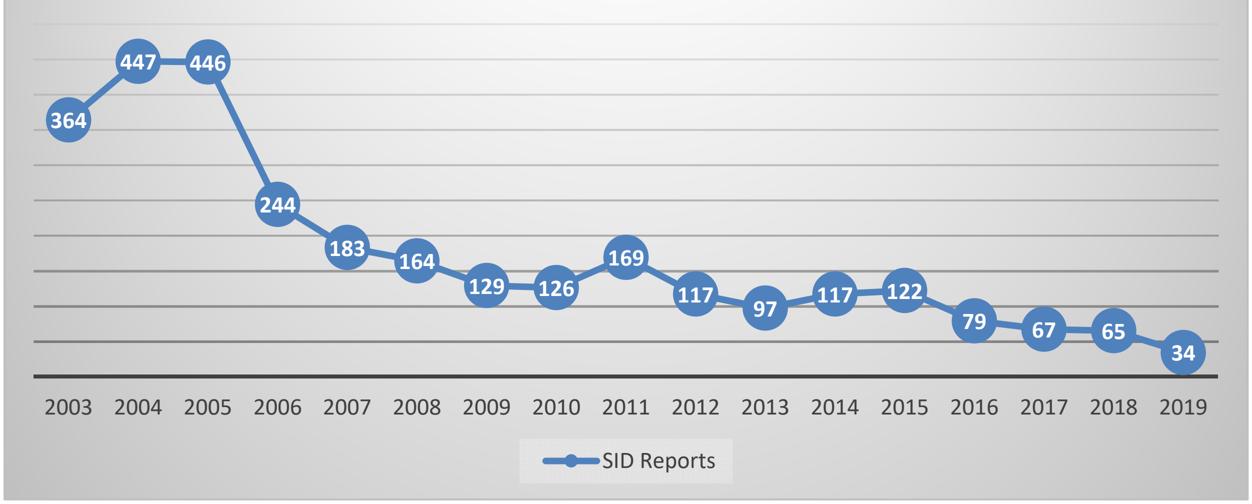
During the period CY 2009 through CY 2015, the average number of annual suspicious activity reports to the NRC remained generally consistent, apart from CY 2011. During this period, the NRC received an average of approximately 125 annual reports, skewed slightly higher by the spike in the number of reports received in CY 2011 (See Figure 1 below). Finally, for the period

[1] The NRC issued initial guidance on reporting suspicious activities in October 2001. The current guidance, IA-04-08, was issued in 2004 and supplements 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.

CY 2016 through CY 2018, the NRC received an average of approximately 70 annual reports. In the first three quarters of CY 2019, the NRC has received 34 suspicious activity reports. In informal conversations with licensees over the last few years on the issue of timely and consistent reporting, some licensees have indicated that they are not submitting reports because of the voluntary nature of the current program. Other licensees have expressed concerns regarding the potential for the suspicious activity reports to be subject to public release under the *Freedom of Information Act* (FOIA). Also based on FOIA concerns, some licensees have chosen not to participate in the voluntary reporting of suspicious activities. Consistent with this anecdotal evidence from licensees, the staff's analysis of the SID database from CY 2014 through CY 2018 indicates that a number of licensees reported no suspicious activities during these years.

Figure 1 - Suspicious Activity Reports per Year (2003-2019*)

(*Year to date through September 2019)



On March 19, 2013, the NRC published the final rule "Physical Protection of Byproduct Material" in the *Federal Register* (78 FR 16922). This final rule added Title 10 of the *Code of Federal Regulations* (10 CFR) 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material." Section 37.57(b) of Part 37 requires licensees possessing category 1 or category 2 quantities of radioactive material to report suspicious activities at their facilities to the local law enforcement agency and the NRC. This superseded the guidance in IA-04-08 for "large byproduct material licensees." As the Commission stated in the Statements of Consideration for the Part 37 final rule, the "reporting of suspicious activities is an important component of evaluating the threat against licensed facilities and material" (78 FR 16947). The Commission further noted that reporting was necessary to determine "whether preoperational activities (i.e., multiple events at a single site or multiple events at multiple sites) may be part of a larger plan and to integrate this information with other agencies in the homeland security and intelligence communities." NRC evaluates each mandatory Part 37 report to determine whether follow-up action is necessary and, if appropriate, shares the report with the FBI and other intelligence agencies.

On November 2, 2015, the NRC promulgated a new cyber security event notification rule (80 FR 67275). As stated in 10 CFR 73.77(a)(3), power reactor licensees are required to report "information regarding observed behavior, activities, or statements that may indicate intelligence gathering or pre-operational planning related to a cyber attack against digital computer and communication systems and networks within the scope of § 73.54." As the Commission noted in the Statements of Consideration for the final rule, "removing the voluntary aspects of reporting certain cyber security events, provides regulatory stability, and ensures the NRC is notified in a timely manner" (80 FR 67267). Such information "could be vital to the NRC's ability to take immediate action in response to a cyber attack and, if necessary, to notify other licensees, Government agencies, and critical infrastructure facilities to defend against a multiple sector (*e.g.*, energy, financial, etc.) cyber attack." *Id*.

In the staff's view, this draft final rule makes mandatory the reporting of the same types of suspicious activities (e.g., intelligence gathering and pre-operational planning) that the Commission has previously indicated are important in protecting NRC licensees and the nation's critical infrastructure. The mandatory suspicious activity reporting requirements in this draft final rule align with the similar mandatory reporting requirements previously approved by the Commission. The staff further notes that on June 20, 2019, the Federal Energy Regulatory Commission approved Reliability Standard CIP-008-6, "Cyber Security - Incident Reporting and Response Planning," (167 FERC ¶ 61,230) for the nation's bulk electric system. This order makes mandatory the reporting of actual or attempted cyber security attacks on entities associated with the bulk electric system (BES). This includes NRC-licensed operating power reactors that provide electricity to the BES.

Use of Suspicious Activity Reports

The staff has determined that a licensee's timely and consistent submission of suspicious activity reports to the NRC, as well as Federal, State, and local law enforcement, is an important part of U.S. government efforts to disrupt or dissuade malevolent acts against the nation's critical infrastructure, including the nuclear sector. Despite the increasingly fluid and unpredictable nature of the threat environment, some elements of terrorist tactics, techniques, and procedures (TTPs) remain constant. For example, attack planning and preparation generally proceed through several predictable stages, including intelligence gathering and pre-attack surveillance or reconnaissance. Pre-attack surveillance or reconnaissance activities can occur as single acts across multiple critical infrastructure sectors, or as multiple acts across a single critical infrastructure sector. Identifying these pre-attack stages offers the NRC, law enforcement and NRC licensee security personnel, a significant opportunity to disrupt or dissuade acts of terrorism before they occur. Suspicious activity reports are one effective tool for maintaining situational awareness of the threat environment and learning about potential malevolent acts directed against NRC licensees. However, to make effective use of suspicious activity reports to disrupt or dissuade potential terrorist attacks, timely and consistent reporting of suspicious activities by licensees to the NRC as well as Federal and local law enforcement is considered necessary.

NRC security staff use suspicious activity reports in the SID database as one factor in analyzing and understanding the threat environment and terrorist TTPs that might potentially affect NRC licensees. For example, from January 2019 through September 2019, NRC security staff queried the SID database 477 times (See Figure 2 below). Trends and changes to the threat environment that might affect NRC licensees are communicated through security advisories and other means. Trends and analysis are also communicated to the Commission, as appropriate. For example, based in part on information obtained from reports of unmanned aerial vehicle (UAV) overflights of NRC-licensed facilities, NSIR staff initiated a study of the potential threat posed by adversary use of UAVs against certain NRC-licensed facilities. The results of this study were presented to the Commission in SECY-19-0102, “Technical Analysis of Unmanned Aerial Vehicles for Nuclear Power Plants and Category I Fuel Cycle Facilities (U),” dated October 15, 2019 (non-publicly available). The SID database is also accessed by other NRC users such as the cyber assessment team.

NRC security staff review and disposition all suspicious activity reports entered into the SID. For example, the staff has identified concerns in several suspicious activity reports and communicated those concerns to the FBI or State law enforcement agencies, as appropriate, for additional follow-up investigations. Although none of these investigations led to criminal prosecutions, follow-up by FBI or local law enforcement agency (LLEA) personnel may dissuade or disrupt potential attacks and heighten sensitivity to the potential risks associated with suspicious activities.

The DHS and FBI continue to view suspicious activity reports from critical infrastructure owners and operators, including the nuclear sector, as key to maintaining situational awareness over these sectors and providing early warning of potential malevolent acts. Figure 2 below demonstrates how often Federal and State agencies access the SID database. From January 2019 through September 2019, DHS has queried the SID database 1,894 times. The FBI has queried the SID database 170 times over the same period. Both agencies have expressed to NRC staff their continued interest in receiving timely and consistent suspicious activity reports. DHS continues to invest information technology resources to update its infrastructure for suspicious activity reporting and communication. Similarly, the Federal Aviation Administration (FAA) has continued to express to the NRC staff a desire to receive timely suspicious activity reports of unplanned aerial overflights of NRC licensed facilities. These reports of aerial overflights are for both manned aircraft and UAVs. State emergency management and law enforcement agencies also query the SID database. From January 2019 through September 2019, State agencies queried the SID database 1,040 times.

This use of the SID database by multiple NRC, Federal, and State users is an indication of the value placed on suspicious activity reports. However, this value could be undermined by the lack of timely and consistent reporting of suspicious activities. The staff has conducted several outreach efforts to licensee security managers and NRC security inspectors to encourage the voluntary reporting of suspicious activities in a timely and consistent manner. Despite these efforts, staff is unaware of any new or enhanced industry initiatives to improve the reporting of suspicious activities to the NRC, the LLEA, or the FBI. The staff believes that making these reporting requirements mandatory will aid in ensuring timely and consistent suspicious activity reporting. In addition, the draft final rule provides licensees with the discretion to reasonably conclude that an activity is or is not suspicious. The supporting regulatory guide, RG 5.87, “Suspicious Activity Reports Under 10 CFR Part 73” (ADAMS Accession No. ML17132A163), provides examples that licensees may use in assessing whether an event rises to the level of a suspicious activity that should be reported. This guidance may decrease reporting of those activities that are reasonably determined not to constitute a suspicious activity.

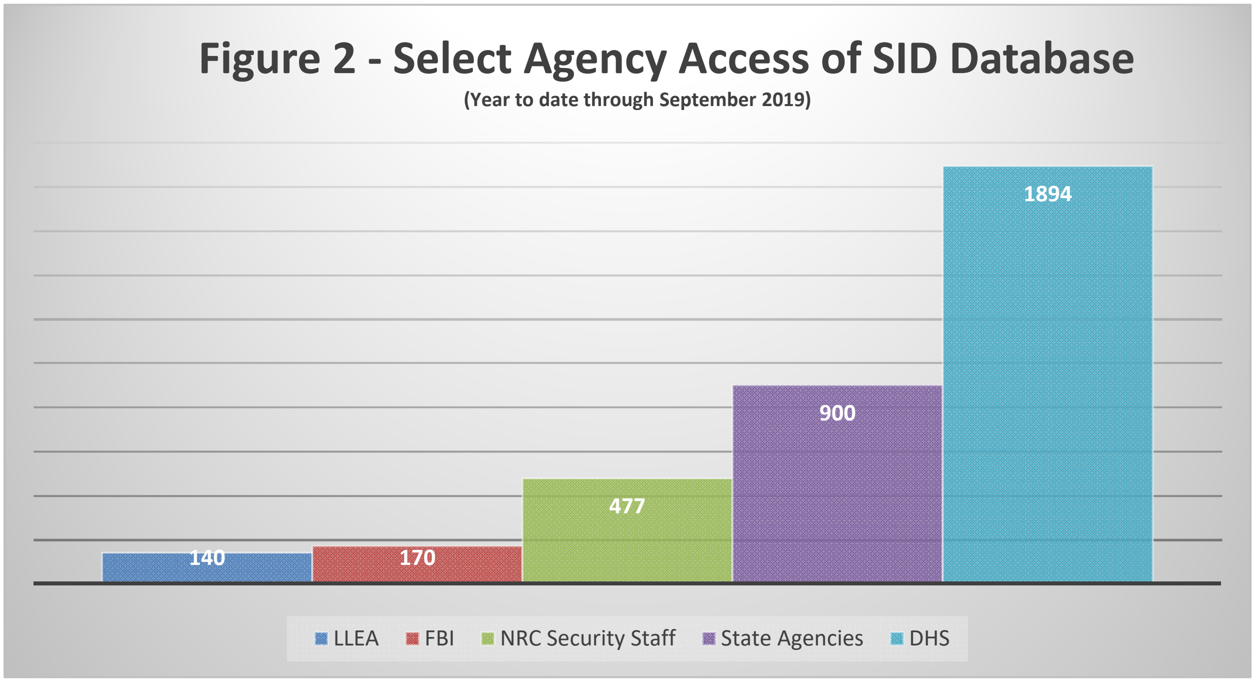


Figure 2 - Select Agency Access of SID Database

(Year to date through September 2019)

Note: For the period January 2019 through September 2019, the SID database was accessed a total of 8,415 times. Figure 2 shows frequent users.

Advantages and Disadvantages of Establishing a Mandatory Reporting Requirement

To support the Commission's evaluation of this issue, the staff has included the advantages and disadvantages of mandatory suspicious activity reporting, below.

Advantages of this new requirement:

- Improves consistency of licensee reporting of suspicious activities to the NRC, LLEA, the FBI, and the FAA (for activities involving aircraft);
- Ensures timely reporting of suspicious activities by licensees;
- Facilitates the NRC's integration of suspicious activities into the threat assessment process, one of the NRC's primary mission essential functions;
- Ensures consistency with the types of existing mandatory reporting requirements in 10 CFR 37.57(b) and 10 CFR 73.77(a)(3);
- Improves suspicious activity reporting on critical infrastructure to Federal intelligence and law enforcement partners, and State emergency management and law enforcement agencies; and
- Promotes regulatory clarity, certainty, and predictability by codifying current industry voluntary efforts into NRC regulations.

Disadvantages of this new requirement:

- Establishes a new reporting requirement for licensees subject to the final rule;

- Imposes a new burden on licensees required to assess and communicate suspicious activity reports in accordance with the final rule;
- Requires licensees to revise or develop suspicious activity reporting procedures and train key personnel on the new reporting requirements; and
- Requires NRC resources to develop inspection and enforcement guidance.

Conclusion

The draft final rule makes the voluntary reporting of suspicious activities mandatory. Mandatory reporting of suspicious activities will increase regulatory stability and also ensure that the NRC receives timely and consistent notification of suspicious activities. Timely and consistent access to this information enables the NRC to maintain situational awareness of the threats to NRC licensees and, if necessary, promptly share this information with our Federal partners in the homeland security and intelligence communities as well as State and local law enforcement. Mandatory reporting of suspicious activities is an important tool that will facilitate U.S. government efforts to disrupt or dissuade terrorist acts. Finally, the mandatory reporting of suspicious activities set forth in this draft final rule aligns with the mandatory reporting requirements previously approved by the Commission.