

Specific Analytical Capabilities

- Security incident trend analysis
- Most common security incident
- Type of incident by location and time frame
- Frequency of incidents by facility
- Most common cause of incidents by type
- Corrective actions applied to incidents
- Timeliness of incident reporting
- Training effectiveness
- Policy effectiveness
- Inter-Complex Incident Correlation

Analysis can be conducted regarding the correlation of incidents that have been, or are, occurring within the DOE Complex. If there is a relationship, this information will assist in determining the root cause, all individuals involved, or potential loss, and support corrective actions.

Policy Effectiveness Assessment

The results of the implementation of a specific DOE policy can be reviewed by querying the ITAC database to identify incidents and root cause analysis results to determine if a policy has been effective in reducing incidents of specific types.

Root Cause Analysis

SO occasionally selects individual inquiries for the ITAC to analyze for specific issues of concern and to examine or conduct root cause analysis. In addition to conducting a circumstance analysis of an incident, the ITAC may also examine the inquiry process itself for investigative sufficiency.



To learn more about the ITAC, or for additional information, please contact:

Michael Schwartz
Manager, Information Security Resource Center
Pacific Northwest National Laboratory
P.O. Box 999, MS K8-58
Richland, WA 99352
Phone: (509) 375-2618
Email: Michael.Schwartz@pnl.gov

ITAC

Incident Tracking & Analysis Center

Incident Tracking & Analysis Center

The DOE Incident Tracking and Analysis Center (ITAC) was established in 2000 to meet the needs of the Department of Energy (DOE) to coordinate, analyze, and archive Incidents of Security Concern. These incidents are events that, at the time of occurrence, have yet to be determined to be a violation of law, but that are of such concern to the safeguards and security program as to warrant immediate reporting, review, inquiry, and subsequent assessment.

The ITAC provides a dynamic collection and analysis capability for current and historical information regarding Incidents of Security Concern. The ITAC conducts circumstance analyses, identifies significant security issues, evaluates root cause analysis, and produces trending information related to Incidents of Security Concern that may provide indicators of continuing or future security concerns facing DOE.

The ITAC supports the DOE Office of Security (SO). Information developed by the ITAC is used to support training courses at the

Nonproliferation and National Security Institute (NNSI) and to provide information and assistance to the DOE Complex.

ITAC Capabilities

The ITAC database is maintained with current security incident information. The information in the database is used to track and trend incident data, and to provide analytical support through queries, database reports, and graphical displays.

This information is used to publish Lessons Learned reports, Crosstalks, and other value-added information for the DOE Complex. The ITAC provides analysis of narrative data contained in the data fields, as well as graphical displays relating to specific security issues, trends, and observations. The ITAC provides trending and analysis of specific incidents as requested by a DOE Operations Office, DOE Contractor, or as determined by SO.

Additional ITAC Support

Reporting Enhancements

The ITAC has developed an Incident-Inquiry Report that provides a standardized electronic format designed to meet the needs of inquiry officials in the DOE Complex, as well as the Security Incidents and

Investigations Unit (SIU). It facilitates accurate, thorough and consistent reporting of information relating to incidents of security concern. This report allows inquiry information to be electronically reported to SO, and facilitates database entry.

Trending Capabilities

By querying the extensive data fields within the ITAC Database, trending can be conducted based on multiple field criteria. Queries may be complex and global, or simple and focused, depending on desired output.

Program Office Support for Damage Assessments

The ITAC can provide analytical information for a specific incident/inquiry, to assist in the identification of potential damage to national security when classified information is, or may be compromised. This analysis capability augments the DOE damage assessment activities.

Lessons Learned

The analysis of specific program elements of an incident provides useful information for the DOE Complex and supports efforts to prevent any recurrence. Lessons Learned may be distributed through various means such as Crosstalks, Website Articles, or Advisories.