Incidents of Security Concern Program Plan

Office of the Chief Safety Officer

Joe Rogers
Fermilab Security Chief

19 July 2021

Revision History

Revision No.	Pages Affected and Description (Original 8/26/2019)	Effective Date
1	Updated FSO to Security Chief	19July2021
2		
3		
4		
5		
6		

Submission and Approval

Submitted by:

Joe Rogers, UID:jrogers Digitally signed by Joe Rogers, UID:jrogers Date: 2021.08.26 09:11:24 -05'00' **8/26/2021**

Joe Rogers, Security Chief
Fermi Research Alliance, LLC
FNAL Environmental, Safety, & Health Section

Date

Reviewed and Approved by:

Amber Kenney Digitally signed by Amber Kenney Date: 2021.08.26 09:18:36 -05'00' 8/26/2021

Amber Kenney, Chief Safety Officer
Fermi Research Alliance, LLC
FNAL Environmental, Safety, & Health Section

Date

Richard K. Verhaagen Digitally signed by Richard K. Verhaagen Date: 2021.10.14 12:18:54 -05'00' 10/14/2021

Rick Verhaagen, Site Office Manager
Fermilab Site Office
Department of Energy

Date

Table of Contents

Attachment

Abbreviations and Acronyms

CFR	Code of Federal Regulations
CHI-ISC	Office of Science Integrated Support Center - Chicago
CIRC	Computer Incident Response Center
CSO	Cognizant Security Office
DOE	Department of Energy
FNAL	Fermi National Accelerator Laboratory
FSO	Facility Security Officer
IOSC	Incident of Security Concern
LEO	Law Enforcement Officer
MI	Management Interest
ODSA	Officially Designated Security Authority
PI	Procedural Interest
PII	Personally Identifiable Information (Intellectual Property)
PPM	Program Planning Management
SAP	Special Access Program
SCI	Sensitive Compartmented Information
SNM	Special Nuclear Material
SO	Security Officer (Fermilab Protective Force)
SSIMS	Safeguards and Security Information Management System
U.S.C.	U.S. Code

1. Purpose

The occurrence of a security incident at Fermi National Accelerator Laboratory (FNAL) prompts the appropriate graded response, to include an assessment of the potential impacts, appropriate notification, extent of condition and corrective actions. For such incidents, Department of Energy Order 470.4B, CRD, Safeguards and Security Program, Att. 5 Incidents of Security Concern, requires a program plan that addresses each component of that policy.

The following plan implements DOE O 470.4B's requirements and definitions.

Incidents of security concern are actions, inactions or events that do the following:

1. Pose a threat to national security interests and/or DOE assets or degrade the overall effectiveness of FNAL's protection program.
2. Create potentially serious or dangerous security situations.
3. Affect significantly the Safeguards and Security Program's capability to protect the lab's safeguard and security interests.
4. Indicate the failure to adhere to security procedures.
5. Reveal that the system is not functioning properly, by identifying and/or mitigating potential threats (detecting suspicious activities, hostile acts, etc.).

Incidents identified require follow up to do the following:

1. Ensure management awareness.
2. Determine the facts and circumstances of the incident.
3. Ensure corrective actions are taken to mitigate the incident.
4. Develop action plans to correct underlying weaknesses and prevent recurrence.
5. Track and trend incidents to improve the health of the security program.
6. Document and determine whether a security infraction or other disciplinary action is appropriate.

The Facility Security Officer is responsible for the following:

1. Develops the IOSC Plan and integrates it with the larger program planning management functions that are outlined in the Site Security Plan (SSP).
2. Assesses and categorizes all incidents, to determine the appropriate level of notification.
3. Reviews all documents generated concerning incidents for classification purposes.
4. Performs tracking and trending analyses on the collective set of incidents for the purpose of monitoring security program performance and to modify security procedures accordingly.
5. Assesses impacts of incidents relative to other site programs and security interests and coordinates, as necessary, with the programmatic element responsible for the information that is compromised or suspected of compromise.

6. Advises the Fermilab Site Office's Officially Designated Federal Security Authority (ODFSA) of adverse trends or other indicators that security plans and/or procedures are not achieving the desired results.

Each IOSC, with the exception of incidents of management interest Category A (see Table 1, on Incident Types, below), requires categorization, an initial report, an inquiry, closure report, and entry into the Safeguards and Security Information Management System (SSIMS). The level of effort associated with the latter three steps is graded based on the incident category and the factors (severity, asset, etc.) surrounding the incident. All information generated as a result of this process must be protected according to its sensitivity and/or classification.

The following considers FNAL's key security categorizations and interests that determine its overall security posture. With the absence of special nuclear material, an unarmed security force, no classified material held on-site, and a small number of cleared individuals, the likelihood of a Security Incident (SI) type incident is limited and more likely to fall into a Management Interest (MI) or Procedural Incident (PI) type incident.

2. IOSC Identification and Categorization

All IOSCs must be categorized by significance level and type. As depicted in the table below, there are three types of incidents (security, management, and procedural) and three levels (A, B, and C).

Table 1. Incident Types, Categories and Response

Incident Type	Event	Required Response
	Security Interest (A). Incidents that meet a designated level of significance relative to the potential impact on the department and/or national security (defined in the subsequent sections), thereby requiring the notification and pertinent involvement of the ODFSA and SECURITY CHIEF. **Security Interest (B)**. Incidents of lesser significance (i.e., incidents that do not meet the Category A criteria) that the SECURITY CHIEF manages and resolves. However, oversight responsibilities remain with the ODFSA.	
Security Interest A	Loss, theft, compromise, or suspected compromise of: (1) Other Accountable Nuclear Materials – DOE-CSC (2) Radiological or chemicals that if misused could endanger the public (3) DOE security badge (PIV-HSPD-12) determined to be the target of theft	(1) Security Officer sends Initial SO Report of Security Incident to FERMILAB SITE OFFICE and Directorate (2) FERMILAB SITE OFFICE sends incident report to DOE-CSC (DOE Office of Science – Consolidated Service Center) (3) DOE-CSC enters incident into SSIMS (4) SECURITY CHIEF enters into IOSC tracking system (Security MFA environment) (5) Following inquiry, SECURITY CHIEF sends Preliminary Report to FERMILAB SITE OFFICE and Directorate (6) SECURITY CHIEF enters corrective actions into Security iTrack (7) SECURITY CHIEF sends Final Closure Report to FERMILAB SITE OFFICE

Incident Type	Event	Required Response
		within 90 days of Initial Report of Security Incident for entry into SSIMS
Security Interest B	Loss, theft, compromise, or suspected compromise of: (1) Export Controlled Information, PII (2) Category 4, Other Accountable Nuclear Material (3) Security key or key card of a protected asset (4) Foreign government material or information that requires reporting based on established agreements and protocols (5) Degradation of security (resulting in site shutdown or Cyber Security function)	(1) SECURITY CHIEF sends Initial SO Report of Security Incident to FERMILAB SITE OFFICE and Directorate (2) SECURITY CHIEF enters into IOSC tracking system (Security MFA environment) (3) Following inquiry, SECURITY CHIEF sends Final Report to FERMILAB SITE OFFICE and Directorate (4) SECURITY CHIEF enters corrective actions into iTrack
	Management Interest: These do not necessarily involve departmental assets but are a unique type of incident that may have potential undesirable impacts. They warrant management notification. They do not require formal inquiry, closure, but still must be categorized - A,B,C	
Management Interest A	Occurrence: (National Security) (1) Fermilab Research is not classified at the National Security level.	(1) SECURITY CHIEF sends Initial SO Report of Security Incident to FERMILAB SITE OFFICE and Directorate (2) FERMILAB SITE OFFICE sends incident report to DOE-CSC (DOE Office of Science – Consolidated Service Center) (3) DOE-CSC enters incident into SSIMS (4) SECURITY CHIEF enters into IOSC tracking system (Security MFA environment) (5) Following inquiry, SECURITY CHIEF sends Preliminary Report to FERMILAB SITE OFFICE and Directorate (6) SECURITY CHIEF enters corrective actions into Security iTrack (7) SECURITY CHIEF sends Final Closure Report to FERMILAB SITE OFFICE within 90 days of Initial Report of Security Incident for entry into SSIMS
Management Interest B	Occurrence: (1) Arrest of an employee on-site (2) Demonstration or protest (3) Willful intrusions (4) Improper access control (5) Willful violation of security procedures/protocols (6) Work stoppages (7) Labor strikes (8) Hostile acts in the workplace (9) External hostile act that jeopardizes on-site safety of personnel (10) Media events (11) Suspicious activity (12) Threats to persons or facilities (13) Confiscated firearms (by LEO) (14) Public demonstrations (15) Civil unrest	(1) SECURITY CHIEF sends Initial SO Report of Security Incident to FERMILAB SITE OFFICE and Directorate (2) SECURITY CHIEF enters into IOSC tracking system (Security MFA environment) (3) Following inquiry, SECURITY CHIEF sends Final Report to FERMILAB SITE OFFICE and Directorate (4) SECURITY CHIEF enters corrective actions into iTrack
Management Interest C	Occurrence: (1) Non-Willful violation of security procedures/protocols (2) Non-Willful intrusions (3) On-Site arrest of a non-employee	(1) SECURITY CHIEF sends Initial SO Report of Security Incident to FERMILAB SITE OFFICE and Directorate

Incident Type	Event	Required Response
		(2) SECURITY CHIEF enters into IOSC tracking system (Security MFA environment) (3) Following inquiry, SECURITY CHIEF sends Final Report to FERMILAB SITE OFFICE and Directorate (4) SECURITY CHIEF eEnters corrective actions into iTrack
	Procedural Interest: These do not necessarily involve departmental assets but are a unique type of incident that may have potential undesirable impacts. They warrant management notification and a look at any potential policy revisions. They do not require formal inquiry, closure, but still must be categorized - A,B,C	
Procedural Interest A	Failure to adhere to security procedures. Unauthorized actions such as: (1) Willful non-compliance with the Fermilab Access Policy / Procedure (2) Willful non-compliance with the Fermilab Site Security Plan	(1) SECURITY CHIEF sends Initial SO Report of Security Incident to FERMILAB SITE OFFICE and Directorate (2) FERMILAB SITE OFFICE sends incident report to DOE-CSC (DOE Office of Science – Consolidated Service Center) (3) DOE-CSC enters incident into SSIMS (4) SECURITY CHIEF enters into IOSC tracking system (Security MFA environment) (5) Following inquiry, SECURITY CHIEF sends Preliminary Report to FERMILAB SITE OFFICE and Directorate (6) SECURITY CHIEF enters corrective actions into Security iTrack (7) SECURITY CHIEF sends Final Closure Report to FERMILAB SITE OFFICE within 90 days of Initial Report of Security Incident for entry into SSIMS
Procedural Interest B	Other actions not resulting in the loss, theft, or compromise or suspected compromise of assets. Examples include: (1) Improper storage of Other Accountable Nuclear Materials and classified materials (2) Improper access controls as outlined in the Fermilab Access Policy / Procedure (3) Improper handling or storage of sensitive and controlled unclassified information (4) Processing information on an unauthorized computer system (5) Unauthorized network-based transmission of information (6) Unauthorized recipient of information (7) Oral or visual transmission of information on an unauthorized communications system (8) Discharge of firearm (9) Introduction of prohibited articles (10) Loss, theft, and unauthorized movement of Other Accountable Nuclear Materials (11) Damages over $10k (12) Non-willful non-compliance with the Fermilab Access Policy / Procedure (13) Non-willful non-compliance with the Fermilab Site Security Plan	(1) SECURITY CHIEF sends Initial SO Report of Security Incident to FERMILAB SITE OFFICE and Directorate (2) SECURITY CHIEF enters into IOSC tracking system (Security MFA environment) (3) Following inquiry, SECURITY CHIEF sends Final Report to FERMILAB SITE OFFICE and Directorate (4) SECURITY CHIEF enters corrective actions into iTrack

3. Inquiry Officials

Inquiry officials may be either federal or contractor employees and must have previous investigative experience or departmental-inquiry official training. Inquiry officials must be knowledgeable of appropriate laws, executive orders, departmental directives and/or regulatory requirements.

Inquiry officials are not authorized to detain individuals for interviews or to obtain sworn statements. They may only conduct consensual interviews and request signed statements. The following outlines the roles and responsibilities of FNAL's designated inquiry official.

1. The SECURITY CHIEF is FNAL's inquiry official as appointed in writing by the Fermilab Site Office.

2. If the SECURITY CHIEF determines or suspects that a foreign power or an agent of a foreign power is involved, the SECURITY CHIEF must stop further inquiry actions and notify the ODFSA, who will assume further notification and reporting responsibilities – to include coordination with the Office of Counterintelligence. In such instances, the SECURITY CHIEF must document the known circumstances surrounding the IOSC and submit all accumulated data to the ODFSA.

3. The SECURITY CHIEF is responsible for conducting the inquiry and maintaining all documentation associated with the inquiry. Specific actions must at least include the following:

    a. Collect all information and physical evidence associated with the security incident. Physical evidence collected must be controlled and a chain-of custody maintained.

    b. Identify persons associated with the incident and conduct interviews to obtain additional information regarding the incident.

    c. Reconstruct the security incident to the greatest extent possible using collected information and evidence. The reconstruction should include a chronological sequence of events that describes the actions preceding and following the incident.

    d. Identify any collateral effect to other programs or security interests.

    e. Analyze and evaluate which systems/functions performed correctly or failed to perform as designed. This action will provide the basis for determining the cause of the incident and subsequent corrective actions.

4. Preliminary Inquiry, Categorization and Reporting Requirements

Employees, Users, and subcontractors must promptly report suspected incidents of security concern to their supervisor and FNAL security as instructed in the Security Awareness Training. The initial reporting is done by the SECURITY CHIEF and may be done telephonically or verbally, or via an email, and must be followed by a formal written report, using the *Initial Report of a Security Incident* template *(*Attachment 1,). The SECURITY CHIEF is responsible for preparing and transmitting the *Initial Report of a Security Incident*. The formal reporting can be accomplished by sending an email, the subject line of which must contain the word "**Incident**." If the template is not used, the information provided in the initial report must correspond to all fields in the template.

The SECURITY CHIEF is responsible to report all IOSCs, no matter the category or severity, to FNAL Directorate leadership and the FERMILAB SITE OFFICE. The SECURITY CHIEF is responsible to ensure that the initial information is communicated to all concerned stakeholders via the most efficient means available. Those means include telephone, email, electronic messaging, verbal brief, and reporting documents both informal and formal as the FERMILAB SITE OFFICE requires or requests.

Preliminary Inquiry

After the *Initial Report of a Security Indicent* is reported, a preliminary inquiry will be conducted. A preliminary inquiry consists of gathering facts to determine if an IOSC has occurred. The SECURITY CHIEF will conduct the verbal interviews, gathering of potential evidence, and documentation of an IOSC. The SECURITY CHIEF coordinates the evaluation of a response to all incidents. After reviewing the suspected incident, the SECURITY CHIEF determines whether it should be handled as either an incident or an administrative matter. If the SECURITY CHIEF determines that sufficient evidence/facts exist to conclude that an IOSC has occurred, the next step is to categorize the incident. If the SECURITY CHIEF determines that an IOSC has not occurred, no further action is required.

The preliminary inquiry and categorization is based on existing policy (usually Fermilab Site Access Policy or Site Security Plan) and any additional criteria as documented in this IOSC program plan.

Preliminary Inquiry reporting and categorization specifications include the following:

1. The "clock starts" when a potential incident is confirmed as an incident of security concern and is brought to the attention of management or security. At that point, FNAL has a maximum of five calendar days to conduct the preliminary inquiry, to make the initial categorization and to perform the initial notification(s). Justification for the categorization (i.e., significance level and type) of the incident should be included in the initial notification.

2. Although a maximum of five calendar days is provided, the incident must be reported by the SECURITY CHIEF as soon as it is categorized. The five-day period provides flexibility for those incidents requiring additional fact gathering, such as a classification review or an inventory check to locate a potential lost/missing item.

3. If, at the five-calendar-day mark, uncertainty still surrounds the incident's categorization, the incident must be reported as a Category A pending completion of the inquiry process. If the final inquiry reveals additional details and facts, the incident can be re-categorized.

Once a decision has been made that an incident is considered reportable under the DOE O 470.4B, the SECURITY CHIEF shall initiate an inquiry – immediately notifying the FERMILAB SITE OFFICE and FNAL Directorate leadership. If the incident is Category A, the FERMILAB SITE OFFICE will ensure the entry of the incident into the Safeguards and Security Information Management System database as notification to headquarters, and the SECURITY CHIEF will enter the incident locally in the IOSC tracking system (Security MFA environment). Category B incidents must only be entered in the local tracking system.

Each security incident must be assigned a unique, site tracking number. The last two digits of the calendar year followed by a unique three-digit number (starting at 001 and progressing chronologically throughout the year) is standard FNAL usage. The incidents are tracked using the IOSC Log located in the Security folder on FNAL's ESH Server1, Security server.

Data Collection

All data/information relevant to the incident shall be collected, such as operations logs, inventory reports, requisitions, receipts, photographs, signed statements, documents, etc. Interviews to obtain additional information shall be conducted. Physical evidence associated with the inquiry should be collected, if available. Examples of physical evidence include recorder charts, computer hard drives, defective/failed equipment, procedures, access logs and readouts from monitoring equipment, etc.

The physical evidence must be protected and controlled, and the FNAL Security Department is responsible to ensure that a chain of custody is maintained.

Specific requirements and actions that must be considered when conducting inquiries include the following:

1. In all instances where the ODFSA disagrees with the FNAL SECURITY CHIEF report, the ODFSA must assume supplemental inquiry responsibilities.

2. When the inquiry into an IOSC necessitates communication with agencies/organizations external to the Department of Energy (e.g., the U.S. Postal Service or FBI or other federal, state or local agency), the ODFSA must be

responsible for performing all such communications. If necessary, the SECURITY CHIEF may perform this function with the ODFSA's written concurrence.

Reporting and Documentation

The FNAL Security Deparment inquiry reports shall describe the conduct and results of the inquiry. Inquiry reports should include an executive summary and a narrative that includes a complete discussion of the facts and circumstances surrounding the incident, including a description of all supporting information, such as the following:

1. Documentation and evidence of information obtained to mitigate the likelihood of compromise of sensitive information or technology.

2. Identification of all personnel involved in the incident, including those associated with the inquiry process, and when they were notified.

3. Identification of the causes of and corrective actions for the incident, and descriptions of mitigating or aggravating factors that may reduce or increase the impact of the incident.

4. Description of the actions that precipitated the incident.

5. Description of all physical evidence, including all records/documents reviewed.

6. Results of any interviews performed, to include copies of any signed statements of involved individuals.

7. Description of actions taken to minimize vulnerabilities created by the incident and prevent further loss/compromise of the security interest.

8. Results of the extent-of-conditions review.

If the incident involves classified matter the following should also be included:

1. A description of the potentially compromised classified matter, including but not limited to classification level, category, caveats and the physical form of the matter. A copy of the evidence or photograph should be maintained and provided to DOE headquarters if requested.

2. The classification guide and topic or source document, including its date.

3. Known recipients of the potentially classified matter.

4. Owner of the classified matter (e.g., program office or other government agency).

5. The reporting organization's conclusion and the basis/facts that support the conclusion and the potential risk to security.

6. The inquiry report, containing supporting documentation of factors used to determine that loss, theft, compromise or suspected compromise did not occur – or that the likelihood of compromise is remote.

The main emphasis for management-interest incidents is on notification; therefore, the subsequent section dealing with inquiries and closure reports is not applicable to this MI type of incident (unless the FERMILAB SITE OFFICE ODFSA requests additional information).

Category-A Preliminary Reporting Requirements include:

1. The FERMILAB SITE OFFICE ODFSA and FNAL Directorate leadership must be notified of all Category A incidents by the SECURITY CHIEF.

2. If the incident involves classified matter, the FNAL departmental element with programmatic responsibility for the information must be identified. Notification must include whether the classified matter originated in another agency or foreign government. A description of the compromised or suspected compromised information must also be included. See Section 8, "Incident Closure," below for additional content considerations for the initial report.

3. If the ODFSA determines that an incident involves the loss, theft, compromise or suspected compromise of top secret, SCI, and/or SAP, the designee(s) or element with programmatic responsibility for the information must review the incident and render two additional determinations as follows.

    a. If it is determined that the incident meets the significant nuclear defense intelligence loss criteria, the appropriate federal entity (or entities) – after consultation with the directors of the CIA and the FBI – must notify Congress. The notification to Congress must occur within 30 days of categorizing the event as a 50 U.S.C. Section 2656 reportable incident.

    b. The element with programmatic responsibility for the information must also determine if the incident warrants a damage assessment.

Category-B Preliminary Reporting Requirements:

While notification and reporting of Category B incidents does not extend beyond the SECURITY CHIEF, it is FNAL's Security Department policy to notify the FERMILAB SITE OFFICE ODSA and FNAL Directorate leadership of all IOSCs regardless of category determination.

Reporting to Cognizant Personnel Security Offices:

Regardless of category, IOSCs may impact an individual's eligibility for access to classified information. Therefore, upon an inquiry's closure, the outcome of the inquiry for all security incidents, regarding individuals applying for or holding a DOE security clearance, must be reported by the ODFSA to the DOE-CSC personnel security office with cognizance over the individual's access eligibility.

Multi-program Reporting:

An event that meets the criteria for reporting as an IOSC does not negate the responsibility for FNAL employees to report through other related reporting chains, such as (but not limited to) the following:

1. Per DOE Order 232.2A, Occurrence Reporting and Processing of Operations Information (January 17, 2017), security incidents that affect both safety and security are reportable through the Occurrence Reporting Processing System.

2. Per DOE Order 151.1D, Comprehensive Emergency Management System (August 11, 2016), security incidents that are reportable under the provisions of this order must continue to be reported in accordance with this order and IOSC.

3. Incidents involving personally identifiable information, both electronic and hard copy, must be reported to the Office of the Chief Information Officer in accordance with DOE Order 206.1, Change 1, Department of Energy Privacy Program and the FNAL Cyber Security Program Plan.

4. Per DOE Order 475.1, Counterintelligence Program (November 1, 2018), the geographically closest element of the Office of Counterintelligence/Office of Defense Nuclear Counterintelligence must be notified of security incidents involving any credible information that a non-U.S. citizen or an agent of a foreign power is involved, or that there are indications of deliberate compromise for a U.S. federal or contractor employee. Appropriate notifications (i.e. FBI) will then be made in accordance with 50 U.S.C. Section 402.a.

5. Per DOE Order 221.1B, Reporting Fraud, Waste and Abuse to the Office of Inspector General (September 27, 2016), when an inquiry surrounding an IOSC establishes information indicating that fraud, waste, abuse, misuse, corruption, criminal acts or mismanagement has occurred, the Office of the Inspector General must be notified.

6. Per DOE Order 205.1C, Change 1, Department of Energy Cyber Security Program (November 1, 2018), all cybersecurity-related incidents must be reported to the Computer Incident Response Center. Any cybersecurity incident involving the loss, theft, compromise or suspected compromise of classified or controlled-unclassified information must also be reported through the IOSC program.

7. Whenever a compromise involves the classified matter of another federal agency, the FERMILAB SITE OFFICE within line management must coordinate with the other government agencies, as appropriate.

8. Whenever a compromise involves the matter of a foreign government that requires protection (e.g., confidential foreign government information modified handling, classified foreign government information), the DOE headquarters within line management must coordinate with the Department of State and the foreign government as appropriate. The foreign government, however, will not normally be advised of any departmental security system vulnerabilities that allowed or contributed to the compromise (DOE Order 470.4B).

9. If a compromise of SCI occurs, the director of the Office of Intelligence and Counterintelligence must consult with the designated representative of the director of Central Intelligence and other officials responsible for the information involved (DOE Order 475.1).

5. Corrective Action

Once causes (direct, contributing, root) are identified, a set of corrective actions are developed by the SECURITY CHIEF to specifically address the causes.

Each cause identified in the causal analysis should have at least one corresponding corrective action. In some cases, it is appropriate for a single action to satisfactorily address more than one cause.

Corrective actions should be as specific as possible, with clearly defined deliverables and due dates that are commensurate with the level of effort required and the urgency needed to complete the action.

Once approved, corrective actions should be tracked by the SECURITY CHIEF to completion in FNAL's local tracking system; Security iTrack. Regular review of action status should be conducted by the SECURITY CHIEF for open actions. In the event that an action will not be completed on time, the action owner should work with the responsible manager to determine if the action plan should be updated to reflect a change in the action activity and/or due date.

All actions, once completed, should be validated by the SECURITY CHIEF. Validation consists of an independent review of the action that assures it was completed. A validation may include an interview of the action owner, review of documentation, spot check of records, or any other activity that demonstrates the action was completed.

6. Incident Trending

Trending of incident data serves two primary purposes: (1) It assists FNAL in identifying programmatic and/or systemic issues that might not be noticeable when data is reviewed separately and independently, and (2) it assists with identifying potential areas of weakness exposed by lesser incidents (precursor activities) before a more significant event occurs.

Noted trends should be shared with the organization from the SECURITY CHIEF, and appropriate actions developed.

The trend analysis should not focus on just the number of incidents. It should include trending of factors such as the types of incidents, responsible organizations, location, dates and causes. The analysis should give contextual consideration to organizational characteristics such as the number of cleared employees, amount and location of classified holdings, types and numbers of classified projects and programs, and other relevant characteristics.

7. Lessons Learned

FNALs security awareness program should work closely with the Office of Communication and the FRA's WDRS - Human Resources training staff to identify topics where the lessons learned – as a result of incidents – can be shared with staff members in a proactive and timely manner, as well as amendments made to future training materials. Every incident should be evaluated for potential lessons-learned material. Also, if deemed appropriate, the development of a lessons-learned article should be included as a corrective action with the concurrence of the Local Insider Threat Working Group (LITWG).

8. Incident Closure

The final closure report serves as the basis for closing incidents. Similar to inquiries, the level of detail provided in the report will vary on the category.

The final closure report for Category A incidents must be submitted within 90 calendar days of preliminary incident notification by the SECURITY CHIEF.

1. Category A incidents must be closed in the Safeguards and Security Incident Management System (SSIMS).

2. Category B incidents can be closed using SSIMS or FNAL's local tracking system; iTrack. The incident notification and the inquiry report must contain supporting documentation of factors used to determine that the likelihood of compromise

and/or the potential for damage to national security is remote (e.g., failure to secure a document in a security container; however, multiple physical protection layers exist preventing unauthorized disclosure). This documentation provides the basis for making a statement that the circumstances surrounding the security incident are such that the possibility of damage to national security can be discounted.

All supporting documentation must be retained by the FNAL Security Department with the final report. For Category A incidents, at a minimum, the documentation must include the following:

1. Material and relevant information (i.e., the "who, what, when and where") providing more detail than contained in the initial report.

2. The name of the individual(s) primarily responsible for the incident, including a record of prior incidents for which the individual(s) were determined responsible. Other involved individuals must also be named. Access authorization levels must be clearly stated if applicable.

3. The report must identify mitigating factors that reduce the potential impact of the incident (such as confirmation that affected computer systems were immediately sanitized) or any other action that reduces the potential impact of the incident.

4. Any aggravating factors that increase the potential impact of the incident (for example, a security container was left unsecured for an undetermined period of time) must be identified.

5. If applicable, documentation noting if the unauthorized disclosure was willful (i.e., intentional vs. inadvertent disclosure).

6. Any corrective actions taken to preclude recurrence and the disciplinary action taken against the responsible individual(s), including retraining must be included in the report.

7. Specific reasons, if applicable, for reaching the conclusion that the theft, loss, compromise, suspected compromise or compromise did not occur or that the likelihood of compromise was remote.

8. Identification of any collateral (i.e., extent of condition) effect to other programs or security interests.

9. If the incident involves the compromise or suspected compromise of information, then the extent of the dissemination (number of individuals and their citizenship, global disclosure via cyber mediums, open-source publications, etc.) must be identified.

10. Identification of specific impacts (i.e., degree of damage, reference 32 CFR Part 2001.48) of the incident to the Department of Energy and/or national security. Whenever an incident involves classified matter or interests of more than one government agency, each agency is responsible for conducting the damage assessment resulting from its compromised matter.

Category B incident reports shall be documented at a level that appropriately captures the situation in the entirety of the event. The report needs to describe the conduct and results of the inquiry, as well as include the following information:

1. Events leading up to the IOSC, and the narrative describing facts and circumstances.

2. Documented evidence obtained that rules out, or mitigates, the likelihood of compromise.

3. Reason for cause.

4. Corrective action, to include disciplinary action, if applicable.

9. Administrative Actions

Whenever possible, the responsibility for an IOSC must be assigned to an individual rather than to a position or office. When individual responsibility cannot be established and the facts show that a responsible official allowed condition to exist that led to an IOSC, responsibility must be assigned to that official.

Security infractions are issued to document the assignment of responsibility for an IOSC. Persons deemed responsible for a security incident may, at management's discretion, be issued a security infraction and/or have disciplinary actions taken in accordance with either DOE's or FNAL's personnel practices as applicable.

Any administrative actions imposed on a cleared individual must be communicated to the respective personal-identity-verification office for Homeland Security Presidential Directive-12.

10. Retention of Files

All paper records associated with FNAL's IOSC program must be maintained for five years by the SECURITY CHIEF.

11. Definitions

1. **Category-A Security Incident**. Incidents that meet a designated level of significance relative to the potential impact on the department and/or national security (defined in the subsequent sections), thereby requiring the notification and pertinent involvement of the ODFSA and SECURITY CHIEF.
2. **Category-B Security Incident**. Incidents of lesser significance (i.e., incidents that do not meet the Category A criteria) that the SECURITY CHIEF manages and resolves. However, oversight responsibilities remain with the ODFSA.
3. **Significant Nuclear Defense Intelligence Losses**. Defined by 50 U.S.C. Section 2656 as "any national security or counterintelligence failure or compromise of classified information at a facility of the Department of Energy or operated by a contractor of the Department that the Secretary considers likely to cause significant harm or damage to the national security interests of the United States."
4. **Compromise**. Evidence is provided that information was disclosed to an unauthorized person or persons (published by media, classified information briefed to uncleared individuals, etc.).
5. **Suspected Compromise**. Evidence is provided that there is a high probability that information was compromised. Although there is no clear indication of compromise, (i.e., no direct recipient), the circumstances associated with the incident indicate that there is an obvious possibility that unauthorized disclosure did occur (classified information is transmitted by email outside of the organization's firewall, classified information is communicated on an unsecure phone line, etc.).
6. **Remote Likelihood of Compromise**. Although protection and control measures are violated, the circumstances associated with the incident indicate that there is a low possibility that information was disclosed to unauthorized personnel (classified information is left unsecured and unattended for a limited amount of time in an area accessed only by personnel with the appropriate clearance level, classified information is transmitted by email inside the organization's firewall and is discovered and isolated within a specified period of time, etc.).
7. **Compromise Did Not Occur**. Evidence is provided that there is no possibility that information was compromised.
8. **Intellectual Property**. A work or invention that is the result of creativity, such as a manuscript or a design, to which one has rights and for which one may apply for a patent, copyright, trademark, etc.
9. **Authorized Person**. A person who has a favorable determination of eligibility for access to classified information, has signed an approved nondisclosure agreement, and has a need-to-know for the specific classified information in the performance of official duties.

ATTACHMENT 1
(Template) Initial Report of a Security Incident

Discovery Date	Discovery Time	Place of Occurrence	Local Number (If applicable)	Incident Number (Assigned by HSIPM)

Incident Category and Type (Check applicable row and fill in type number)		Interest Type (SI or PI)	Category (A or B)
	Information Protection (Complete supplementary section below)		
	Protective Force/Executive Protection		
	Physical Security		
	Program Management Interest		
Are Foreign Nationals Involved? (Check Yes or No.)		Yes	No
Is Media Interest likely? (Check Yes or No.)		Yes	No

Brief **UNCLASSIFIED** Description of Incident. (Classified details, if needed, must be sent separately.)

CAUTION – Details of Security Incidents may be classified – Check with a Classifier before completing.

Describe the initial steps taken to mitigate the incident (information systems have been sanitized, documents secured, etc.)

Supplement for Information Protection Incidents								
What is the highest level and category of Information involved?								
Classification Level	Top Secret		Secret			Confidential		
Classification Category	RD		FRD			NSI		
Do any Special Caveats apply? (Check all that apply)								
WD*	SCI	SAP	WFO	FGI	OGA	NOFORN	Other	
*WD, Weapon Data, is information in Sigma 14, 15, 18 or 20 as defined by DOE O 452.8.								
For Controlled Unclassified Information (CUI) – insert type								
What organization has programmatic responsibility for the information?								

Program Office and HSIPM Determinations		
Does the incident constitute a, "Significant Nuclear Defense Intelligence Loss," requiring Congressional Notification per 50 U.S.C. Section 2656?	Yes	No
Is a formal Damage Assessment warranted?	Yes	No

Point of Contact (Person Making Report)		
Name	Organization	Phone

OFFICIAL USE ONLY (When Filled In)
May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), exemption numbers and categories: (6) Personal Information, (7) Law Enforcement. Department of Energy review required before public release.
Name/Org: _____ Date: _____

Official Use Only (When Filled In)