SEMD-SD-RO-213 – Security Risk Assessment (SRA) Procedure (FARE Assessment Process)

1. Purpose

The purpose of this procedure is to provide guidance when Security Department personnel conduct Security Risk Assessments (SRA). The Fermilab Asset Risk Evaluation (FARE) Assessment is Fermilab's SRA process.

2. Scope

This procedure applies to all Security personnel with adequate authority responsible for providing physical assessment functions mentioned above.

3. Applicability

This policy applies to all uniformed members of the Fermilab Security Department, full-time and part-time employed by Fermi Research Alliance (FRA) for Security Services

4. Effective Date and Date Reviewed/Updated

This policy went into effect on September 14, 2020 and its update was effective on February 1, 2024.

5. Policy

The function of physically conducting assessments on every building on the Fermilab site, by the Security Department, is an important element to the security operation of the Laboratory. This task contributes to the Laboratory's ability to provide a safe and secure environment for employees and visiting scientists to work and live in.

6. Security Department Detailed Procedure:

Table 1 Consequence Assessment	High	Medium	Low
Accelerator/Physics Shutdown	>30 days	3-30 days	<3 days

Major Project/Activity Delay	>100 days	10-100 days	<10 days
Additional Cost	>$300k	$30-$300k	< $-30k
Injury or Illness	Death, substantial disability, or serious overexposure	Some disability or slight overexposure	No disability or overexposure
Environmental Impact or Damage	Widespread and long-term	Localized and long-term or widespread and short-term	Localized and short-term

Table 2 Access vulnerabilities	High	Medium	Low
Attractiveness	Target and/or its contents are very critical /desirable	Target and/or its contents are fairly critical/desirable	Target and/or its contents are not very critical/desirable
Accessibility	Ready access – no barriers, people directed next to targets	Some access – few or partial barriers, people can get to targets	Poor access – multiple barriers, people diverted away from targets
Susceptibility	Minimal effort required to affect target, tools unnecessary	Some effort required to affect target, hand tools effective	Great effort required to affect target, powered equipment or energetic reaction
Visibility	Target areas difficult to observe, observers normally absent. Including Parking Areas.	Target areas partially obscured, observers occasionally present. Including Parking Areas.	Target areas readily observable, observers normally present. Including Parking Areas.

Table 3 Recovery Potential	High	Medium	Low
Recovery Potential	< 3 days	3-30 days	>30 days

Table 4 Protective measures	High	Medium	Low

Barriers	Concrete walls, inaccessible windows, few doors, good repair	Sheet metal, wood frame, good repair. 6' or higher in good repair	Light construction, standard construction in poor repair
Occupancy	Always staffed	Normal work hour staffing	Seldon/intermittently staffed
Patrols	3 or more rounds/shift. High visibility at night outside. To include parking lot	2 rounds/shift. Decent visibility at night outside. To include parking lot	<2 rounds/shift. Poor visibility at night outside. To include parking lot
Intrusion Detection System (IDS) & Video Assessment and Surveillance System (VASS)	Multi-layer system (perimeter, space and target protection) More than 3 cameras	Multi-layers (perimeter and space protection) 1-2 cameras at this location	Single layer system (perimeter protection) no cameras at this location
Physical Access Control System (PACS)	Low and Medium features coupled with Security camera presence.	Alarm linked to FIRUS	Access and Reporting. Key Access only

Table 5 Risk Factor Classification	Other Accountable Nuclear Material (OANM)	Property Protection Area (PPA) or Red / Yellow Technology Areas	Laboratory Infrastructure	Major Laboratory Program / Project / ect.	Other Fermilab Buildings
Risk Factor Totals	≥ 120 points; Asset loss would have a high impact on the Security / Safety of employees and the community AND is also moderately vulnerable.	100+ points; Asset loss would have a high impact on the mission of the lab, these are the most monetarily valuable areas of the lab, contain sensitive security information AND is also moderately vulnerable.	80-99 points; Asset loss would have a significant impacts on how the laboratory operates. Loss of these areas could result in a shutdown of the laboratory.	60-79 points; Asset loss could have a high impact on mission BUT is not very vulnerable. OR- Asset loss could have a moderate impact on mission AND is moderately vulnerable.	< 59 points; Asset loss could have a moderate impact on mission AND is not very vulnerable.

Table 6 Adjusted Risk Rating	Need additional protective measures	May need additional protective measures	Protective Measures are adequate
Adjusted Risk Ratings	< 59 points The physical protection system is generally believed to not be effective against the defined threat.	60-119 points The physical protection system is generally believed to be somewhat effective against the defined threat.	≥ 120 points The physical protection system is generally believed to be effective against the defined threat.

Table 7 Generic Threat	Description	Type
Terrorist	The objective of the threat may vary widely and may include infliction of damage to infrastructure, property, or equipment and seizure, destruction, or use of a nuclear weapon, and/or chemical or biological agent. Capable of committing acts such as theft, bombing (including use of large vehicle bombs or aircraft), extortion, facility seizure, hostage taking, kidnapping, and sabotage (including CBR).	Outsiders
Criminal, Individual	An individual who seeks classified and/or sensitive unclassified information or material, nuclear material, or government property for the purpose of gaining economic advantage or attempts to alter data maintained by DOE or attempts to steal or embezzle government funds or commit contract fraud for the purpose of economic advantage to the individual or the individual's employer. May have access to classified matter, SNM, and/or security areas.	Outsiders/ Insiders
Criminals; Organized	Persons who conspire, and/or perpetrate criminal acts against DOE or DOE contractors for profit or economic gain. Prone to commit acts such as theft, fraud, extortion, and coercion.	Outsiders
Mentally Ill	Capable of committing acts such as arson, bombing, extortion, facility seizure, sabotage (including CBR sabotage), and attacks against individual employees or threats to do such to accomplish personal goals. May have access to a facility's most sensitive activities.	Outsiders/ Insiders
Disgruntled Employee	Normally willing to commit crimes posing low-risk of detection such as vandalism, work interruption, property destruction, arson, bombing (including the use of pre-positioned vehicle bombs), theft of Government property, theft, or destruction of classified and/or sensitive information or material, and industrial sabotage, but may commit crimes with unacceptable adverse consequences, such as espionage/foreign intelligence collection, radiological, and/or chemical sabotage.	Insiders

Violent Activists	Using tactics such as demonstrations, facility seizure, theft, sabotage (includes CBR sabotage), individual targeting, and civil disobedience.	Outsiders
Intelligence Collector	Attempts to collect classified, sensitive unclassified, proprietary, economic, scientific information, and/or other targets of opportunity. May have legitimate access to Departmental facilities, possibly including security areas, due to his employment status and access authorization or membership in a foreign inspection team.	Insiders

7. Fermilab Asset Risk Evaluation Process

7.1 The major steps of the asset risk evaluation process include:

7.1.1 Identify asset to be evaluated.

7.1.2. Complete Asset Risk Evaluation.

Consequence Assessment (Table 1)

Access Vulnerability (Table 2)

Recovery Potential (Table 3)

Security protective measures (Table 4)

7.2. Evaluate Risk Factors Total

Assets rated as High Risk (≥120) are OANM / PPA

Assets rated as High Risk (100+) are PPAs with Red, PII, CUI

Assets rated as Medium Risk (80-99) are PPAs - Laboratory Infrastructure

Assets rated as Medium Risk (60-79) are PPAs - Major Laboratory Projects

Assets rated as Low Risk (<59) do not require categorization and are rated "Other Assets" Or GAAs.

7.3. Evaluate Adjusted Risk Rating

Assets rated as High Risk (≥120) have adequate protective measures in place.

Assets rated as Medium Risk (60-119) may require additional security protective measures. Enter into iTrack and assign/develop corrective actions.

"Other Assets" rated as Low Risk (<60) require additional security protective measures. Enter into iTrack and assign/develop corrective actions.

7.4 Detailed Procedure

Using the Fermilab Asset Risk Evaluation spreadsheet, see sample below, and subsequent following tables, determine the risk factor total and adjusted risk rating for each asset. Assets whose risk factor total 100 points, or more are at high risk and should be considered a PPA. Risk factor totals between 60 and 99 points should be considered a Major Laboratory Project or Fermilab Infrastructure. Total points of less than 60 are low risk and do not require security countermeasures, these are classified as "Other Fermilab assets." PPAs and OANM must be noted in the Site Security Plan.

- Identify asset to be evaluated.
- Complete Asset Risk Evaluation.
- D/P Subject Matter Experts (SMEs) complete:
- Consequence Assessment according to Table 1.
- Access Vulnerabilities according to Table 2.
- Recovery Potential according to Table 3.
- Security Department complete:
- Security protective measures according to Table 4.
- Evaluate Risk Factors Total Table 5.
- Assets rated as High Risk (≥100) are PPA.
- Assets rated as Medium Risk (60-99) are a PPAs - Major Lab Project / Fermilab Infrastructure.
- Assets rated as Low Risk (<59) do not require categorization and are rated "Other Fermilab Assets."
- Evaluate Adjusted Risk Rating (Table 6).
- Assets rated as High Risk (≥100) may have adequate protective measures in place.
- Assets rated as Medium Risk (60-99) may require additional security protective measures. Enter into iTrack and assign/develop corrective actions.
- "Other Laboratory Assets" rated as Low Risk (<59) require additional security protective measures. Enter into iTrack and assign/develop corrective actions.

- Update the Site Security Plan with the results of the Asset Risk Evaluations.
- Repeat every five years or as activities/mission change.
- Physical Security Guard Requirements

High	120+	100% Physical Inspection. Go inside each room of each building. Assess all doors. Adequate outside lighting. Scan FELIX barcode, radio communication with the SOC.
Medium	119	100% Physical Inspection. Inspect each main corridor of each building. Assess all doors. Adequate outside lighting. Scan FELIX barcode, radio communication with the SOC.
Medium	60	
Low	59-	Conduct outside 360◦ walk around. Scan FELIX barcode, radio communication with the SOC.

Commented [MAL1]: Look at this.

The FSO is responsible for overseeing the following functions are completed:

- Physical Security Checks are completed on all structures onsite each shift to ensure all doors are physically locked based on the following priorities:
- Other Accountable Nuclear Material (OANM / PPA) Areas
- Property Protection Areas (PPA)
- Laboratory Infrastructure / Major Laboratory Projects
- Zones 1-8 (in that order)
- Main Campus (Wilson Hall, LINAC, Booster, LSC)
- Industrial Complex (IARC, FCC, ICB)
- Fixed Target Area (NML, CMTF, Meson, Proton)
- Neutrino, Muon Campus Area (SBN, Minos)
- Site Services (Site 29, 37, 38, 40, RCPF)
- Main Injector Area
- Main Ring Area (D0, Site 55)
- Village complex

*Continue using FELIX wands where applicable during Min Safe

*While conducting Security Checks, spot checks of individuals is imperative to ensure those that are on site are supposed to be.

The Security Protective Force is responsible for communicating the following to the Security Operations Center:

- All buildings left unsecured and identified during Security Checks
- Results of any negative inspections (rates of inspections 1-5) at Control Point 3 for Fermilab Property Passes during Min Safe Operations

The Security Operations Center is responsible for the following:

- Adding Security Protective Force messages related to unsecured buildings to the Security Operations Center Blotter
- Watching-out for any abnormal occurrences on the security cameras and notifying the Security Protective Force
- Ensuring that the proper messaging is sent to the Campus Access Office in order to notify the Fermilab residents of the change in Batavia Gate hours; closing early at 2130 hours.

8. Definitions

8.1 COO – Chief Operating Officer. Provides operational guidance for Fermilab Safeguards & Security.

8.2 FSO – Facility Security Officer is in charge of managing security for Fermilab's facilities. Responsible for creating a secure environment for employees, vendors, and Fermilab visitors. Manage daily activities regarding entry, video security, and other security devices.

8.3 SSIWG – Safeguards and Security Interface Working Group

8.4 An Asset is a Fermilab and Fermilab leased space facilities, construction projects, experiments, scientific projects (e.g. DOE O 413.3b), and equipment. Fermilab does not have any Security Assets or Security Interests.

8.5 A Fermilab Asset Risk Evaluation (FARE) is the process by which an asset is evaluated to determine if it is a security risk. The evaluation determines if an asset is a Property Protection Area (PPA), or not categorized. It also determines if adequate security protection measures are in place to properly secure the asset, see Appendix A. The FARE is Fermilab's process for incorporating and conducting a Security Risk Assessment (SRA).

8.6 A Security Risk Assessment (SRA) is an evaluation of potential threats against a safeguards and security interest and the development of potential security countermeasures to address vulnerabilities. It also provides Fermilab with a firm foundation on which to make informed decisions regarding the effectiveness of a safeguards and security system. Incorporates Red, Yellow, and Green areas that are depicted in the S&T Matrix, Export Controlled information, Personal Identifiable Information (PII) or Intellectual Property, CUI, Trademarks, and areas where Other Accountable Nuclear Materials are stored. Scoring ranges from 0 – 135.

8.7 Credible Threats to Fermilab are mission disruption, theft, hostage, protest.

8.8 A Property Protection Area (PPA) is an area where the consequences of some adverse, intentional act might destroy DOE property and result in significant and prolonged programmatic impacts to the HEP program. Asset risk evaluation/Risk Factor totals ≥ 60 points shall be defined as PPAs due to the security risk associated with the asset, see Table 5.

8.9 A General Access Areas (GAA) Asset risk evaluation/Risk Factor totals 59 points and below shall be defined as a GAA, due to the security risk associated with the asset. These areas / buildings may not have a card access system but will be locked.

8.10 The Consequence Assessment is an evaluation of the credible threats to a specific asset and assessing five potential impacts (listed below) also see Table 1. Each consequence is weighted and noted in parentheses. The weight, rated on a scale from 1-5 (low to high) is meant to represent the relative impact of a given factor to high energy physics program. The impacts include:

- Accelerator or physics shutdown (5)
- Major project or activity delay (4)
- Recovery costs (4)
- Injury or illness (3)
- Environment or public image impact (2)

8.11 Access Vulnerability is an evaluation of the credible threats applied to a specific asset and assessing four potential vulnerabilities (listed below) and see Table 2. Each vulnerability is weighted and noted in parentheses. The weight rated on a scale from 1-5 (low to high) is meant to represent the relative impact of a given factor to high energy physics program. The vulnerabilities include:

- Target attractiveness (2)
- Target visibility (2)
- Target susceptibility (2)
- Target accessibility (2)

8.12 Recovery Potential is an evaluation of the length of time an asset would need to recover from a worst-case scenario, credible threat security incident.

8.13 Protective Measures are security countermeasures in place at the time of completing the Asset Risk Evaluation spreadsheet or recommended based upon the Adjusted Risk Rating. Each protective measure is weighted and noted in parentheses:

- Perimeter (3)
- Occupancy (3)
- Patrols (4)
- Intrusion detection system (4)
- Proximity Card Access (3)

8.14 The Adjusted Risk Rating is the result of completing the Security Risk Assessment Spreadsheet: it is a post-mitigation risk ranking. Adjusted Risk Rating scores are organized into High, Medium, or Low risks to determine when additional protective measures may be warranted.

- High: Adjusted Risk Rating ≥ 120 points → current protective measures are adequate.
- Medium: Adjusted Risk Rating 60 – 119 points → additional protective measures may be needed.
- Low: Adjusted Risk Rating < 59 → additional protective measures are required as soon as possible.

9. Responsibilities

9.1 Facility Security Officer – is the author of this procedure and will ensure it is maintained. The FSO is also responsible for providing coordination efforts to SSIWG staff on compliance of this procedure. The Facility Security Officer is also responsible for ensuring each facility, outdoor construction site, and critical infrastructure are evaluated at least every five years, or as activities or mission needs change to assure adequate security countermeasures are in place.

9.2 Security Department Supervisors – are responsible for ensuring that the Security Risk Assessment (SRA) / FARE Assessment is conducted and followed, and this procedure is shared with the Security Operations Center and the Protective Force personnel.

9.3 Building Managers – are responsible for posting mandatory signage at all the main entrances of each building. This signage will be given to them by the Facility Security Officer.

9.4 The Security and Emergency Management Division is responsible for completing the Security Risk Assessment Spreadsheet for all Fermilab facilities and other areas.

9.5 The Division, Section, and Project Heads are responsible for providing data regarding facility, program and operations information in order to complete the evaluation.

10. Authorities

Site Security Plan (SSP)

11. Owner

The Physical Security Manager is the owner of this policy.

12. Review Cycle

This policy shall be reviewed annually or more frequently, as needed.

13. Communication Plan

The requirements of this policy shall be communicated by the Physical Security Manger to all Security Department personnel, and periodic training shall be provided. This policy shall be available in the Fermilab Security Department policy database.