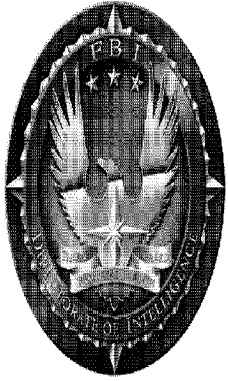


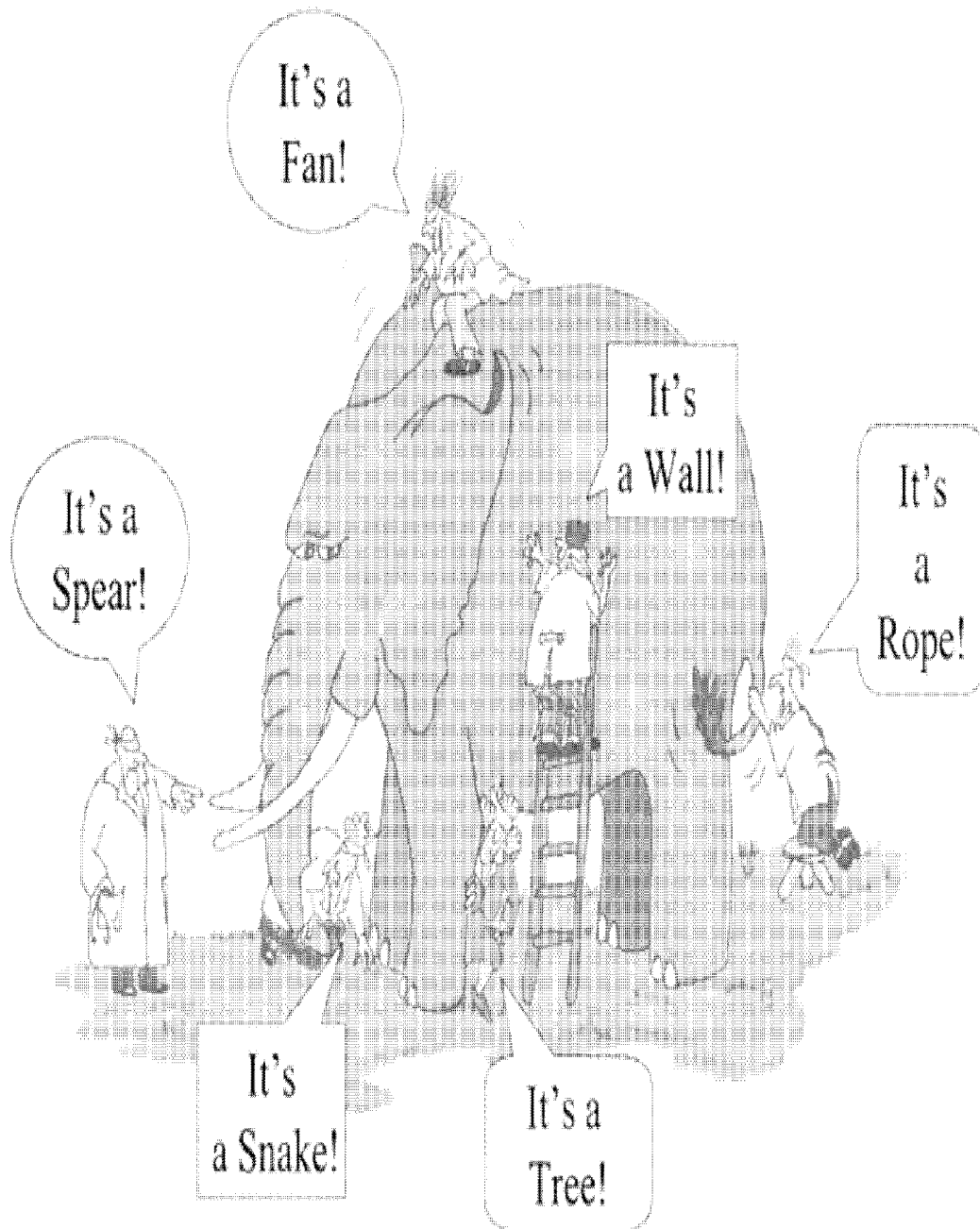
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 03-07-2012 BY 65179 DMH/BAW/STP/RYS

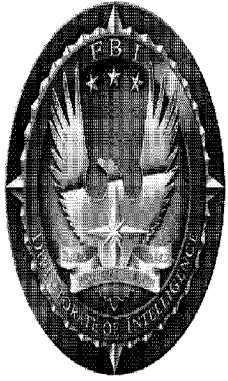


Domain and Collection Management



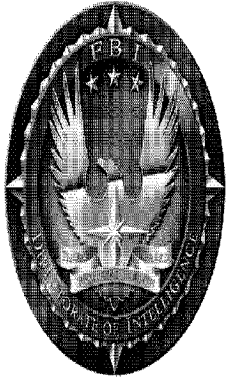
What is your Domain Perspective?





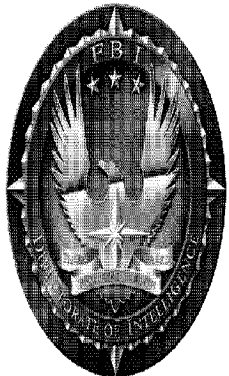
Domain Management

The goal of Domain Management is to develop a comprehensive understanding of an Area of Responsibility's (AoR) threats and vulnerabilities, so that intelligence gaps may be filled, resources effectively deployed, and threats anticipated and mitigated

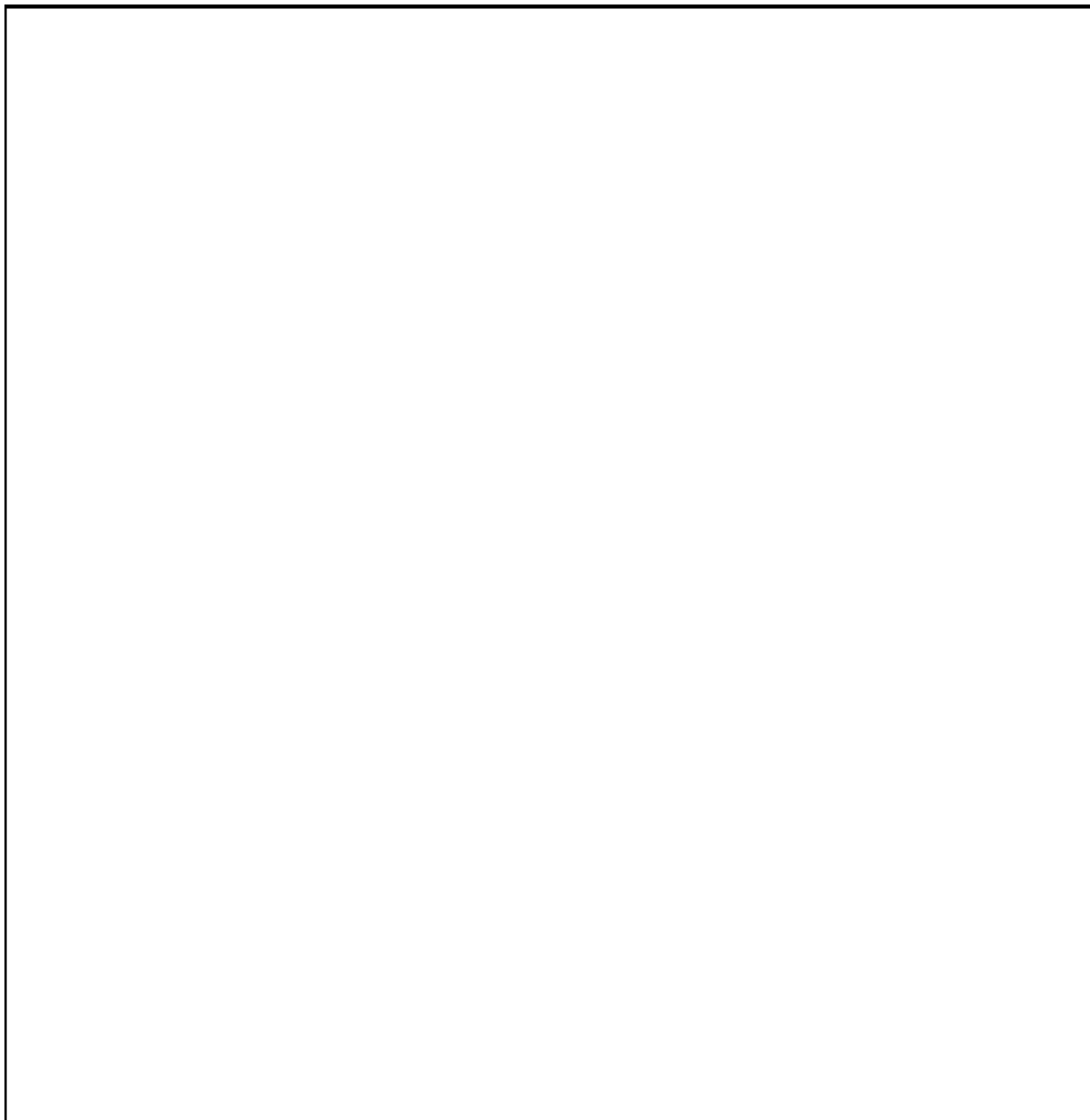


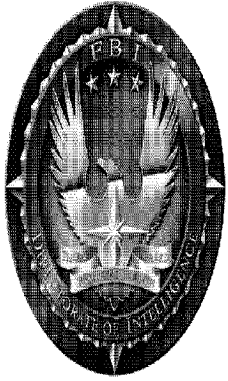
What Framework Do You Use?

1. **Intent:** Activity, risk
2. **Capability:** Physical means, knowledge, sophistication, association
3. **Vulnerability:** Target richness, access, defenses
4. **Criticality:** Violence, impact, public trust



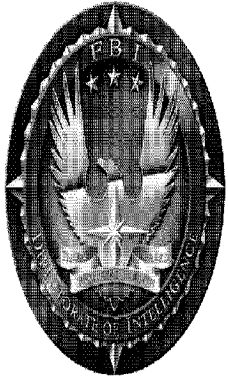
DM Tools and Technology





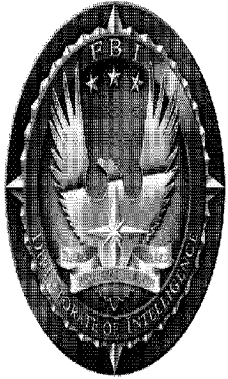
Collection Management

The process of receiving and converting intelligence needs and gaps into questions (Requirements), prioritizing how those questions will be answered, assigning the questions to collectors for resolution, and tracking the progress.



24 National Threat Priorities

- Determined by the operational division Assistant Directors.
 - Are pursuant to the Director's Priorities, but do not replace the eight investigative program priorities.
- Specific threats for which the FBI needs to have focused intelligence collection.
- Collection against each threat priority will enable the FBI to develop a comprehensive, national perspective on threats to national security.



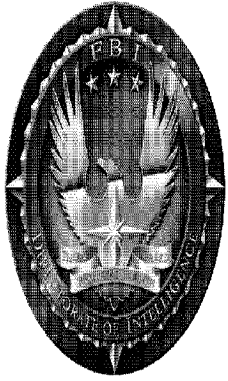
Threat Mitigation Team

- A business process for field offices to consistently, systematically, and proactively develop a strategy to address and mitigate field office prioritized threats and FBI national priorities

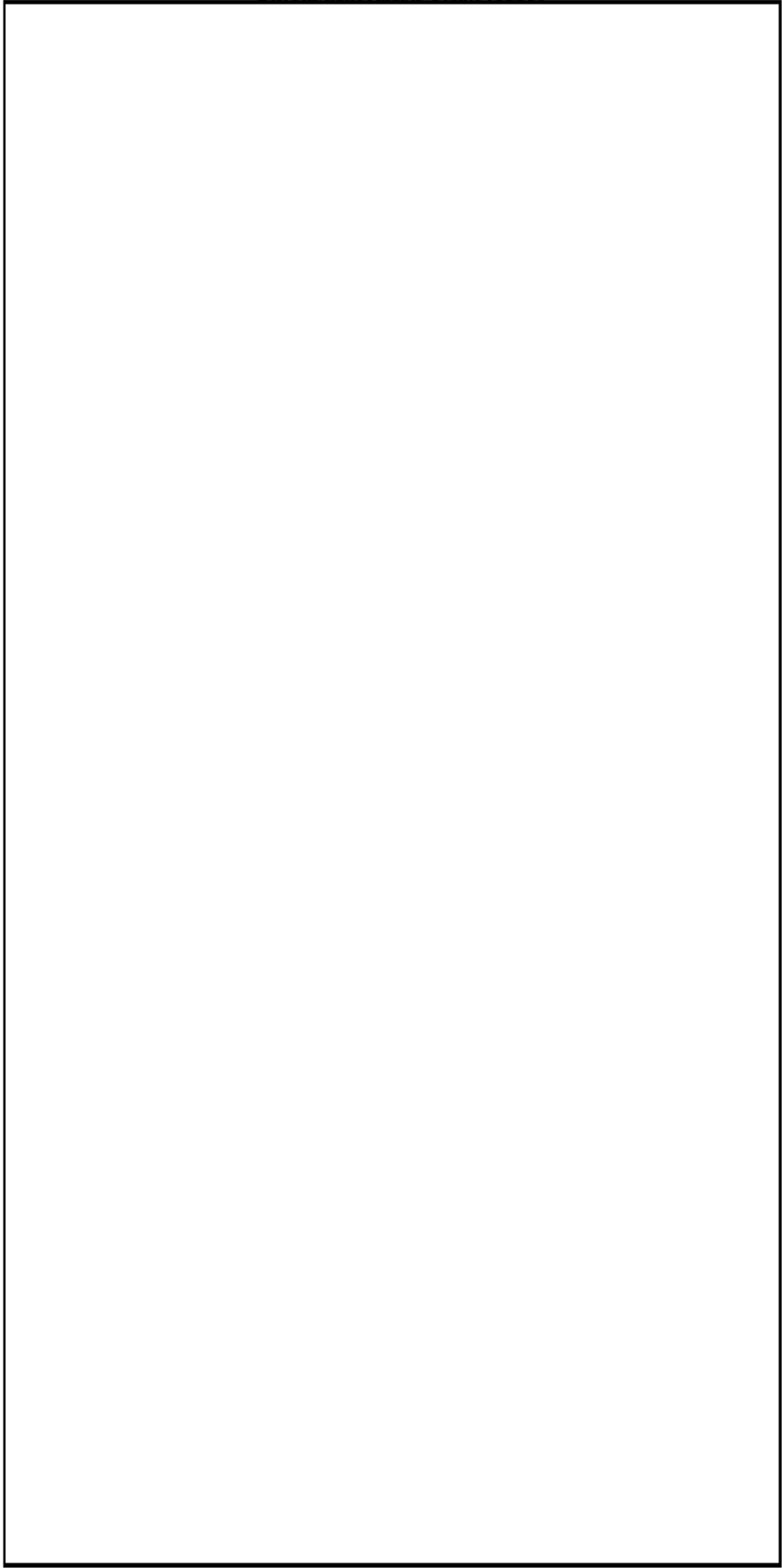
When Should TMT Be Used?

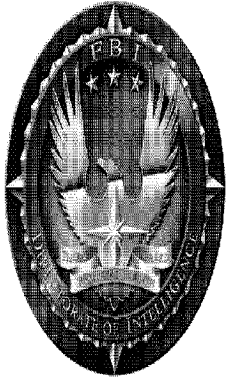
- Field office prioritized threats
- National threat priorities
- Response to Collection Emphasis Messages
- Emerging threats





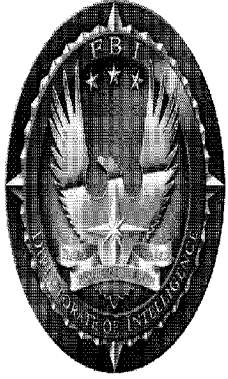
Threat Mitigation Team (TMT)





Threat Mitigation Strategy (TMS)

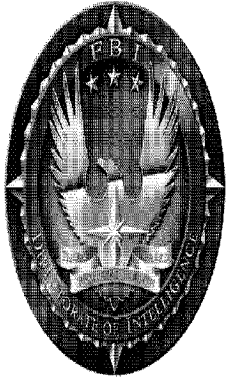
- I. Threat to be addressed
- II. Domain Overview
- III. Collection Capabilities
- IV. Prioritized Gaps
- V. Investigative Cases
- VI. Intelligence Plan
- VII. Investigative/Operational Plan
- VIII. Resources
- IX. Limitations
- X. Leads



What are Assessments?

- Non predicated investigations
- Do not require “particular factual information”
- Require an authorized purpose
- Can NOT be based solely on exercise of First Amendment protected activities

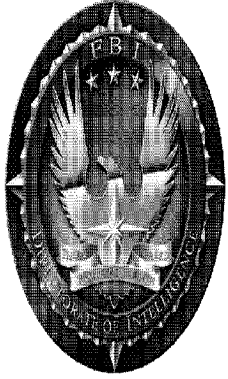
UNCLASSIFIED//FOR OFFICIAL USE ONLY



Type 3 Assessments

- To identify and obtain information about potential targets of or vulnerabilities to criminal activities in violation of federal law or threats to the national security.
- *Opened to address an identified threat.*

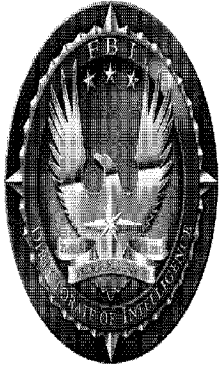
UNCLASSIFIED//FOR OFFICIAL USE ONLY



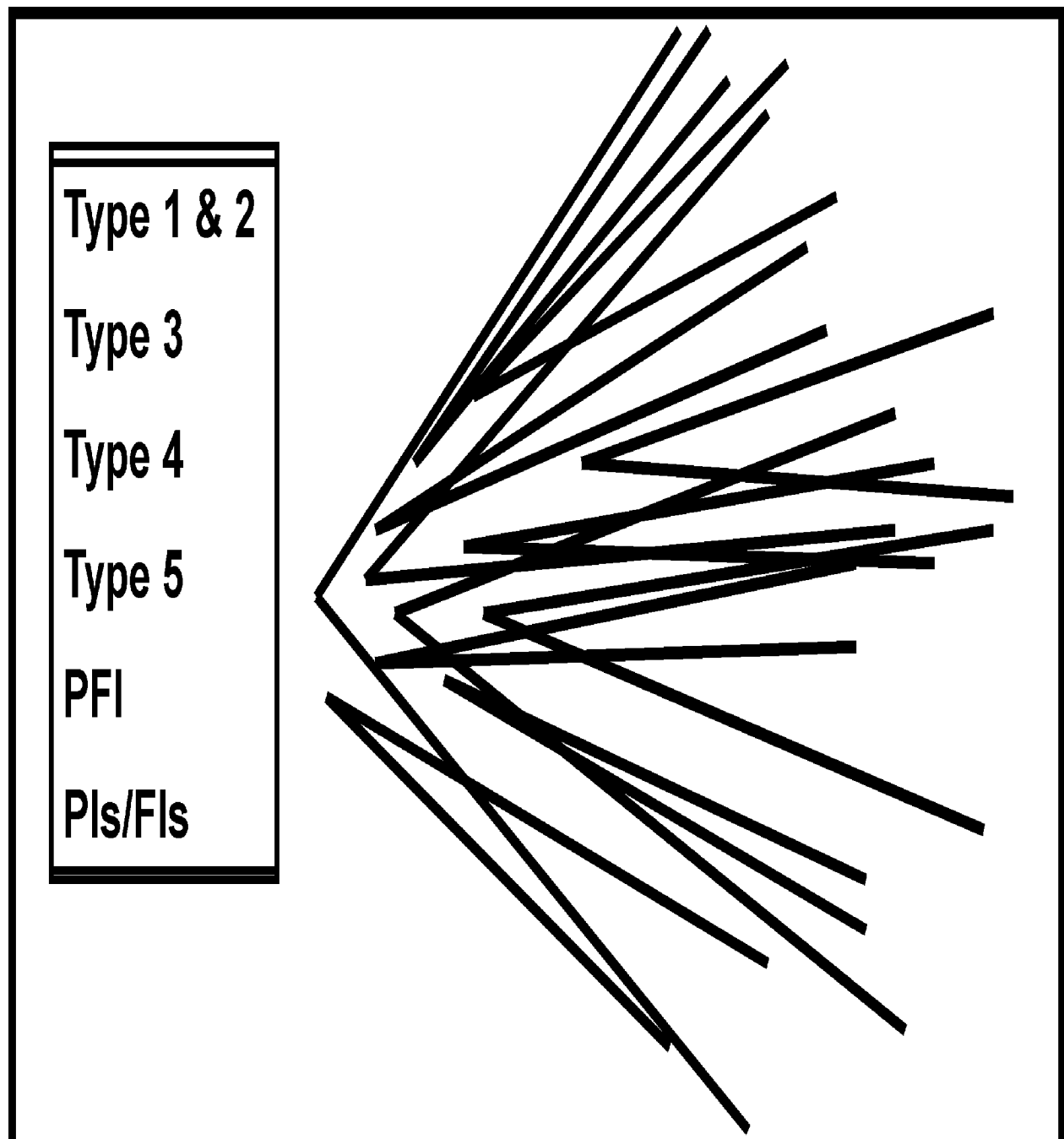
Type 4 Assessments

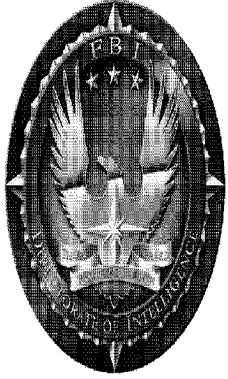
- To obtain information to inform or facilitate intelligence analysis or planning.
- *Does the threat exist in my AoR?*

UNCLASSIFIED//FOR OFFICIAL USE ONLY



Addressing the Threat





Questions?