DoD Reportable Thresholds and Insider Threat Assessment

COGILITY

Contents

List of Figures

List of Tables

BLUF (Bottom Line Upfront)

The purpose of this white paper is to explore the alignment of a framework currently in use by insider threat assessment tools, such as Cogynt, a Continuous Intelligence Platform from Cogility, with reportable thresholds defined by the DoD Insider Threat Management and Analysis Center (DITMAC) and to recommend steps or possible analytic solutions that may facilitate meeting the DITMAC reporting requirements. The 13 reportable thresholds are described and compared with other insider threat knowledge base constructs (Threat/Risk Behaviors and Potential Risk Indicators used by the Department of the Air Force Insider Threat Hub). To address the complex mapping between these various constructs, two approaches are described. First, a decision tree framework is illustrated to outline steps needed to identify applicable reportable thresholds for a reported case; a shortcoming of this approach is that it requires additional judgments to address queries of interest at a finer granularity than is provided in the threshold definitions. Next, an updated hierarchical framework is proposed to accommodate the 13 thresholds directly in the Cogynt knowledge base, including more fine-grained sub-categories for thresholds of interest. The framework suggests that a pattern-based model incorporating a PRI-to-Threshold mapping may be used not only to identify and characterize associated Reportable Thresholds but also to model and assess threat levels of observed cases. The paper concludes with a brief discussion of research recommendations.

Introduction

In 2016, the Under Secretary of Defense for Intelligence and Security (USD[I&S]), who serves as the DoD senior official responsible for overseeing the DoD Insider Threat Program, established DITMAC within the Defense Counterintelligence and Security Agency. Validated by all DoD components, this guide, intended for insider threat professionals working at DoD component programs, identifies insider threat events that merit enterprise level awareness and analysis. The Reportable Thresholds guide recognizes that some events may not clearly meet the enterprise level requirements of any threshold, while other events may meet multiple thresholds. In all cases, DITMAC relies on the good judgment of component program leadership and staff expertise to make appropriate determinations regarding incident reporting. Therefore, two key factors supporting the threshold determination are (a) whether the behavior directly or potentially threatens DoD personnel, resources, or capabilities; and (b) whether the behavior is aberrant to the culture/context in which it occurred. Concerning behaviors that do not meet the enterprise level reporting threshold are best managed at the component level and, therefore, do not merit DITMAC reporting.

Ultimately, the insider threat assessment process is dependent upon expert judgment. Computer-based decision support systems have been and are being developed to support this process, with varying levels of maturity. To help program leadership and expert analysts meet DITMAC reporting requirements, additional decision support is needed to “correlate” the observed cases with the DITMAC Reportable Thresholds. This is challenging because the insider threat/behavior types of concern that are enumerated at the component level do not align entirely with the 13 DITMAC thresholds.

A leading decision support system developed by Cogility Software embodies the more ambitious “whole person” concepts that are evident in the 13 Thresholds. This system, called Cogynt, is a continuous analysis decision platform that employs Hierarchical, Complex Event Processing (HCEP) to implement a pattern-based approach to threat assessment. Cogynt is currently being tested at the Department of the Air Force Insider Threat Program (DAF C-InTP) Hub in San Antonio, Texas. Insider threat decision support tools rely to a varying extent on Potential Risk Indicator (PRI) knowledge bases and are typically structured around that taxonomic foundation. For example, Cogynt is built upon a combination of a DoD PRI taxonomy and an extensive/comprehensive ontology called SOFIT (the Sociotechnical and Organizational Factors for Insider Threat ontology) [1].

The purpose of this white paper is to explore and recommend steps or possible analytic solutions that may be incorporated into insider threat assessment tools, such as Cogynt, to align them more closely with the DITMAC reporting requirements.

Background

DITMAC Thresholds

The 13 DITMAC Reportable Thresholds are as follows:

1. **Serious Threat** – posing a reasonable risk to life or limb, or the potential to degrade or destroy a critical DoD capability.
2. **Allegiance to the United States** – exhibiting questionable allegiance to the U.S. through words or actions (including involvement or support/advocacy of any act of sabotage, treason, or sedition).
3. **Espionage/Foreign Considerations** – individuals suspected of using their authorized access to commit espionage on behalf of a Foreign Intelligence Entity (FIE).
4. **Personal Conduct** – reflecting intentional deception in an official process, such as concealing or falsifying relevant facts from security investigations, or a pattern of behavior that brings the individual's character (judgment, trustworthiness, honesty) into question.
5. **Behavioral Considerations** – exhibiting behaviors that cast doubts on an individual's judgment, reliability, or trustworthiness; or psychological factors such as emotional stability and paranoid, bizarre, antisocial, or aggressive behavior.
6. **Criminal Conduct** – investigation, arrest, or apprehension by a federal, state, or local law enforcement agency; or conviction, indictment, or charging for crime involving loss of life; or actual or suspected acts or threats of violence – including sexual assault, criminal offenses involving weapons or explosives, or illegal possession/transfer of weapons of mass destruction.
7. **Unauthorized Disclosure** – knowing involvement in unauthorized disclosure, theft, loss, or compromise of classified or protected information.
8. **Unexplained Personnel Disappearance** – suspicious death or unexplained disappearance of any covered person (holding a TOP SECRET or TOP SECRET/SCI clearance).
9. **Handling Protected Information** – deliberate mishandling of protected information or exhibiting a pattern of negligent noncompliance with rules, procedures, guidelines, or regulations for protecting such information.
10. **Misuse of Information Technology** – deliberate misuse of information technology or exhibiting a pattern of negligent noncompliance with rules, procedures, guidelines or regulations pertaining to information technology.
11. **Terrorism** – providing support to, or being in contact with, known or suspected domestic or international terrorist or extremist individuals, organizations, or groups; or any attempt/conspiracy to commit terrorism.
12. **Criminal Affiliations** – providing support to, or being in contact with, known or suspected domestic or international criminal organizations, street gangs, or groups engaged in racketeering; or any attempt/conspiracy to conduct such activities.
13. **Adverse Clearance Actions** – documented suspension, revocation, or denial of a security clearance for reasons identified in thresholds 1-12.

Because Threshold 13 likely results from one or more instances of other thresholds, it is in some respects redundant with the other Thresholds, and it might be aptly characterized instead as a PRI Role Type (Precipitating Event), as defined in SOFIT [1][3].

DAF Threat/Behavior Types

The DAF C-InTP Hub defines eight threat types, described below and in Table 1.

- **Data Exfiltration** – Any unauthorized movement of secured data to unauthorized domains or cross domain boundaries.
- **Sabotage** – A deliberate act or acts with the intent to injure or interfere with or obstruct the national defense of a country by willfully injuring, destroying, or attempting to destroy any national defense or mission material, premises, or utilities, to include human and natural resources.
- **Misuse of Privileged Access** – Deliberate actions that undermine the integrity of trusted or privileged access.
- **Workplace Violence** – Physical and psychologically damaging actions, violence, or threat of violence against colleagues, associates, or leadership. It can occur at or outside the workplace and can range from threats and verbal abuse to physical assaults and homicide.
- **Suicidal Ideations** – Suicidal thoughts, or suicidal ideation, means thinking about or planning suicide. Thoughts can range from a detailed plan to a fleeting consideration. It does not include the final act of suicide.
- **Espionage** – The act of obtaining, delivering, transmitting, communicating, or receiving information in respect to the national defense with an intent or reason to believe that the information could be used to the injury of the United States or to the advantage of any foreign nation and not pursuant to an international agreement duly entered into by the United States.
- **Unintentional Insider Threat** – Non-malicious, negligent, accidental, or uninformed activities or actions exhibited by entities that present an inadvertent risk.
- **Maladaptive** – Non-criminal and non-violent activity that does not meet established standards of acceptable or clinically healthy behavior.

Table 1. Correspondence Between Insider Threat Behavior Types and DITMAC Thresholds

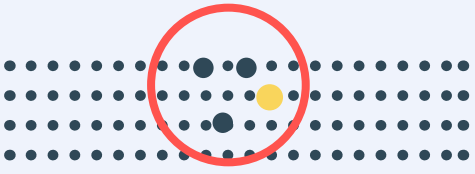
Threat/Behavior Type	Source	Potential Correspondence with DITMAC Thresholds												
		1	2	3	4	5	6	7	8	9	10	11	12	13
Data Exfiltration	SOFIT	✓	✓	✓				✓		✓	✓	✓	✓	✓
Sabotage	SOFIT	✓	✓	✓		✓	✓		✓	✓	✓	✓	✓	✓
Workplace Violence	SOFIT	✓	✓			✓	✓					✓	✓	✓
Unintentional Insider Threat	SOFIT				✓	✓				✓	✓			✓
Fraud	SOFIT						✓				✓		✓	✓

As is shown in the table, each of the threat behaviors potentially relates to multiple DITMAC Thresholds. 11 of 26 Personal Predispositions, 92 of 119 Behavioral Precursors, and 70 of 107 Technical Precursors.

Insider Threat Potential Risk Indicators (PRIs)

There are several hundred PRIs. We are currently in the process of integrating a DoD list of PRIs and the list of about 270 PRIs documented in the *Sociotechnical and Organizational Factors for Insider Threat (SOFIT)* knowledge base [1][2]. The final, integrated list is likely to contain up to 300 PRIs.

Fig. 1 shows the relationships between the DITMAC Reportable Thresholds and the DAF C-InTP insider threat/behavior types (graphically depicting the information in Table 1), as well as the links between the DITMAC Thresholds and many lower-level PRIs (the PRI collection shown here is not exhaustive due to the large number of PRIs). The PRIs are color-coded to reflect four main categories defined in the SOFIT [1][3] Role Type taxonomy (which was inspired in part from Shaw's Critical Pathway framework [5]): *Personal Predisposition* (reflecting psychological/personality factors), *Behavioral Precursors*, T*echnical Precursors* (relating to Threshold 10), and *Precipitating Events.*



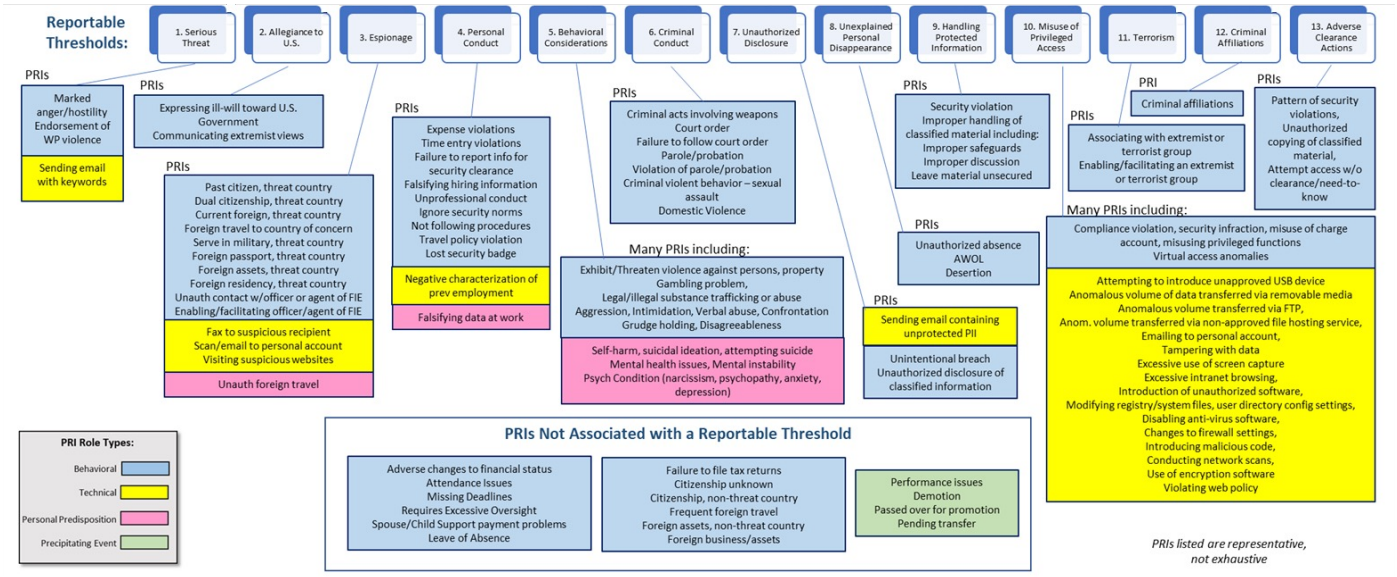


Figure 1. Relationships Between Reportable Thresholds, Behaviors, and PRIs

Unlike the Threat/Behavior types that link to multiple DITMAC Reporting Thresholds, the PRIs tend to map to only one Reporting Threshold; however, some PRIs do not relate to any of the Thresholds. This is because the SOFIT ontology – and the DAF C-InTP approach – embrace a proactive mitigation philosophy that seeks to identify potential risks before they become (reportable) cases. Therefore, PRIs and collections of PRIs that do not meet DITMAC reporting thresholds are still recognized and of interest in this component-level insider threat program.

Because the mappings between individual PRIs and Thresholds are unique, a decision support tool for reporting of Thresholds may be best informed by examining associations between observed PRIs and Thresholds. However, this is complicated by the fact that a typical insider threat case comprises multiple PRIs, which still may map to different Thresholds. The challenge increases if management queries concern cases that fall into sub-categories of Thresholds that are not necessarily recorded. Therefore, responses to management/stakeholder queries (such as the number and types of Thresholds reported per month, or the number of sexual assaults within the Criminal Conduct Threshold) will still require additional effort – even the need to re-visit a case and apply expert judgment to enumerate sub-categories. To alleviate this problem, additional decision support and recording is needed. The next section considers possible avenues for pursuing decision support solutions.

Decision Support Concepts for Identifying Reportable Thresholds

This section of the paper describes possible approaches to designing and building analytic support into Cogynt that will recommend relevant DITMAC Reportable Threshold(s) that best align with cases identified in Cogynt.

Decision Trees

A useful "top-down" approach is to document decision analysis steps to classify a case according to the Reportable Thresholds in a decision tree. There are numerous instantiations of decision trees depending on the order in which one "attacks" the problem. Figure 2 depicts one example of a preliminary decision tree that covers Thresholds 1-12. The figure shows the decision points as solid blue diamonds; the Reportable Thresholds are indicated as white circles. Also shown in the diagram are the Threat Behaviors listed in Table 1—these are identified as colored rounded rectangles.

As noted earlier, the Reportable Thresholds apply only to cases that have been referred (e.g., via DSOS, the "DITMAC System of Systems") for further investigation. The first step considers whether the case, which comprises a set of observed PRIs, includes a psychosocial concern. If so—and particularly if it does not fit into other Thresholds—it may be classified into Threshold 5 (Behavioral Concern), which can include suicidal ideation or several other (non-criminal) behavioral or psychosocial issues, including the Maladaptive behavior type. As has been pointed out in DITMAC material describing the Reportable Thresholds and Adjudicative Guidelines, it is not uncommon for cases to bridge multiple Thresholds.

The next step inquires if the case represents an act that has occurred, an unexplained disappearance, or a threat of future action. If it represents a threat, it maps to Thresholds 1, 2, or 12 depending upon whether it represents a threat to harm persons or property (Threshold 1); a threat of sabotage, treason, or sedition against the U.S. (Threshold 2); or criminal affiliations (Threshold 12). If it represents an act, then the Threshold type depends on four characteristics (noncompliance, theft, sabotage, or violence) concerning the nature of the act: If it represents noncompliance, then the choice of threshold depends upon whether the lack of compliance reflects not following procedures (leading to Threshold 4, Personal Conduct) or misuse of information technology (Threshold 10, Misuse of IT); or security violations (which leads to Threshold 9, Handling Protected Information). Alternatively, the act might involve theft, sabotage, or violence. If theft is involved, the question is whether it represents disclosure of sensitive information. If not disclosed, then Threshold 4 (Personal Conduct) is appropriate; if the data exfiltration is disclosed and it is performed by a threat actor with ties to a foreign adversary, then the exploit is considered

Threshold 3 (Espionage). If no ties to foreign entities are observed, then this is considered an individual act representing Threshold 7 (Unauthorized Disclosure).

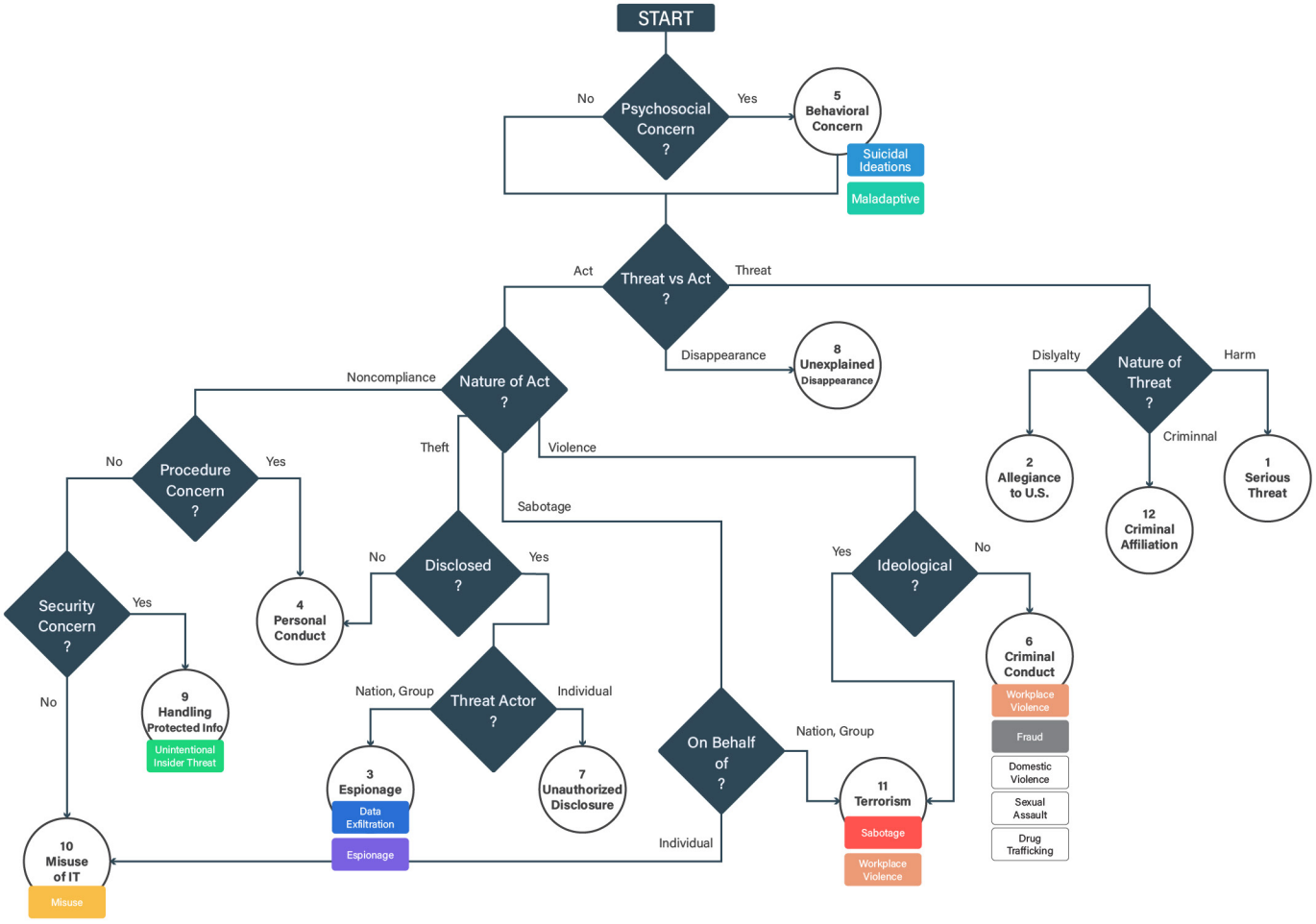


Figure 2. Proposed Decision Tree for Identifying Thresholds

Decision points shown as solid blue diamonds. DITMAC Thresholds shown as white circles.
Threat Behaviors shown as colored rounded rectangles (corresponding to those in Figure 1 and Table 1).

Going back to the nature of the act, if it is sabotage, then it would be classified as Threshold 10 (Misuse of IT) if it was done by/for an individual without foreign adversary connections; if the sabotage is conducted by an individual on behalf of an adversary, then it is best identified as Threshold 11 (Terrorism). Finally, if the nature of the act concerns violence, then the threshold determination depends upon whether an ideology is involved. Violence by individuals espousing domestic extremism, religious extremism, or political violence reflects Threshold 11 (Terrorism); otherwise, it represents Threshold 6 (Criminal Conduct).

A disadvantage of the decision tree method is that it does not provide a straightforward means of identifying cases that match two or more thresholds. Examples of so-called “cross-threshold” cases are provided in Table 2.

- A case involving domestic violence will be reportable under the Personal Conduct threshold if it includes intimidation or controlling behaviors; if it goes beyond intimidation and involves physical violence, it will likely also be reportable as Criminal Conduct.
- A case involving identification with violent extremism will fall into the Serious Threat threshold, but if it includes statements or behaviors that reflect violent extremist ideology, it will also be reportable under Threshold 2, Allegiance to the U.S. If the behavior brings harm to other individuals or to institutions, it will also fit the definitions of Criminal Conduct and Terrorism.
- A case involving suspicious or criminal financial activity (such as racketeering, fraud) would be reportable under Threshold 4 (Criminal Conduct). Instances in which delinquent finances are associated with concerning behaviors (e.g., gambling) would also raise concerns under Threshold 4 (Personal Conduct) or Threshold 5 (Behavioral Considerations). If the behavior includes international financial transactions or business activities, it will be reportable under Threshold 3 (Espionage).

Table 2. Examples of Cross-Threshold" Cases that May be Reportable Under Multiple Thresholds

General Topic Area	Description	Applicable Thresholds
Domestic Violence	Intimidation/harm to family member could involve threats of or actual physical violence or violations of privacy, limiting access to communication, finances, social contacts	4. Personal Conduct 5. Behavioral Considerations 6. Criminal Conduct
Violent Extremism	Identification with or support for violent extremist or hate-based ideology, such as contact with violent extremist groups; procurement or possession of violent extremist literature; threats or harassment reflecting violent hate-based ideology	1. Serious Threat 2. Allegiance to the U.S. 4. Personal Conduct 6. Criminal Conduct 11. Terrorism
Financial Considerations	Financial criminal activity such as racketeering, identity theft, bribery, fraud; unreported foreign assets/business/contacts	3. Espionage 4. Personal Conduct 5. Behavioral Considerations 6. Criminal Conduct

To address the problem of multiple thresholds, the decision tree can be expanded; however, it is likely to become unwieldy and difficult to use. An alternative approach is described in the next section.

Bottom-up / Hierarchical Approach to Identify Reportable Thresholds

When a case potentially maps to multiple reportable thresholds, the analyst may choose to indicate each of the relevant thresholds, but this is not appropriate when reporting distribution statistics such as the occurrences of different thresholds over time or across locations. Therefore, generally, a judgment is required about which reporting threshold best matches a case. In contrast to the top-down approach embodied in the decision tree method described above, a bottom-up method based on associations between PRIs and Thresholds may provide a more direct means of selecting the most appropriate reporting threshold.

For DITMAC reporting purposes, for any given case we can report the Threshold with the highest counts, or alternatively, we can select/report the Threshold that reflects the greatest level of concern. To implement this method, we may define a new Reportable Threshold *taxonomy* within the PRI knowledge base that includes not only the thirteen classes of thresholds, but also sub-classes that reflect more detailed criteria or characteristics. An illustrative Threshold Taxonomy is shown in Figure 3.

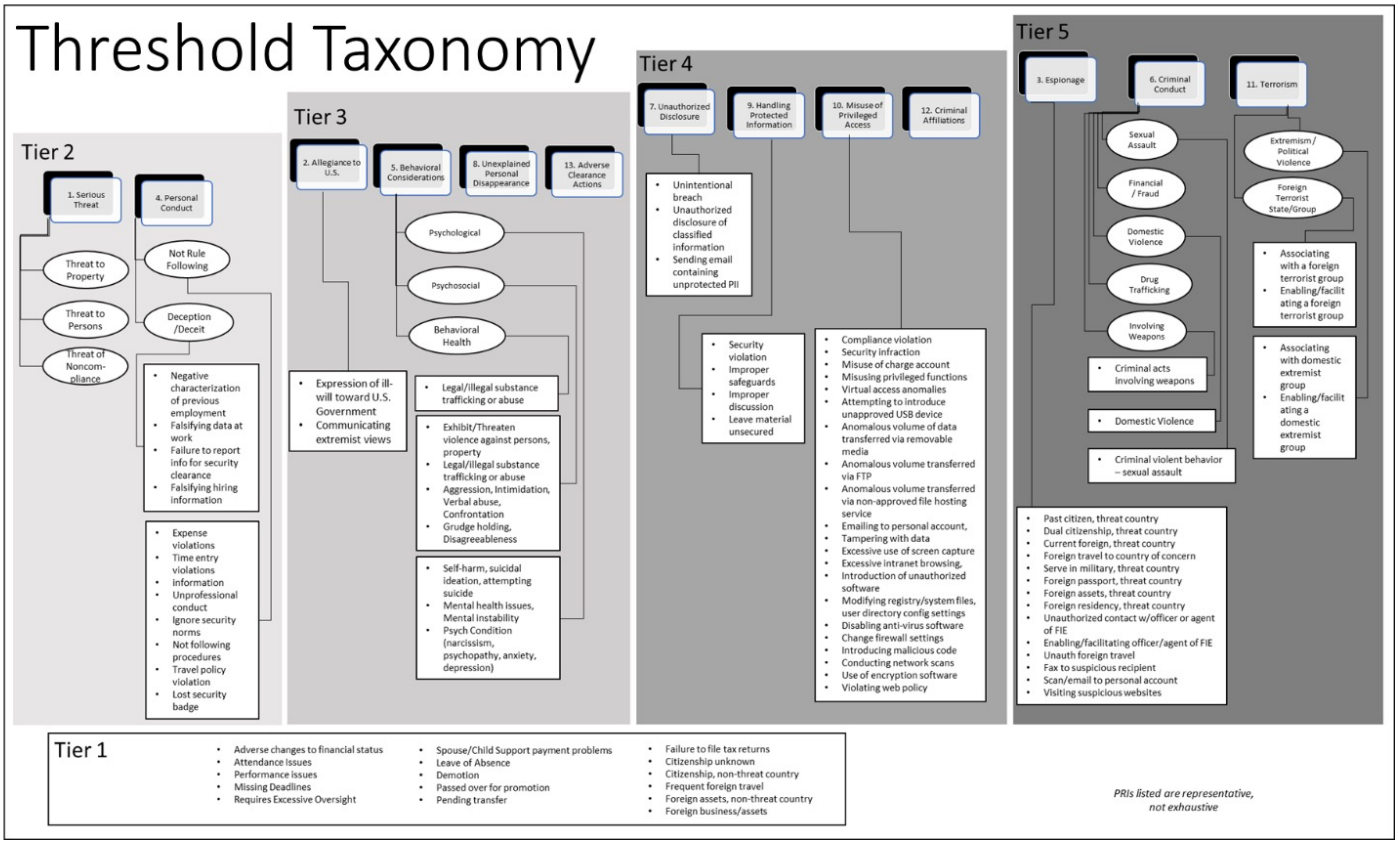


Figure 3. Threshold Taxonomy Showing Sub-Classes of Interest

The figure depicts the taxonomy organized into five tiers that contain patterns of PRIs that are increasing in concern or severity.

- Tier 1 comprises the PRIs that are not directly associated with any of the thresholds – as described previously, these relate to general concerns or contributing factors that may suggest potential/future risk but are not reportable by themselves (or even in combination with one another). It is reasonable to suggest that observing one or more Tier 1 PRIs along with PRIs in other Tiers will tend to increase the threat/risk of a case.
- Tier 2 includes four Reportable Thresholds that are of concern, but not as serious as others in higher tiers. Observing Tier 2 PRIs in addition to Tier 1 and/or other Tier PRIs will, similarly, tend to increase the threat/risk of a case.
- Tier 3 specifies four Thresholds that are of significant concern, including those associated with issues of allegiance to the U.S. and behavioral considerations.
- Tier 4 includes four Thresholds that are of high concern such as those associated with unauthorized disclosure, mishandling of protected information, and criminal conduct/affiliation.
- Tier 5, the highest level thresholds, comprises three Thresholds that represent very high or grave concerns such as espionage, criminal conduct including violent acts, and terrorist acts.

To illustrate the method, consider the following examples. In Case 1 (Table 3), four PRIs are observed that fall into three Reportable Thresholds: Demotion (not associated with a Threshold) is in Tier 1(Figure 3) and is associated with a Very Low concern level; *threatening behavior*, associated with Threshold 1-Serious Threat, is in Tier 2 with a Low concern level; two PRIs—*aggression/verbal abuse* and *violence against person* are in Threshold 5-Behavioral Considerations, at Tier 3 with Medium concern. In this example, the selected Reportable Threshold is 5-Behavioral Considerations, since it is the highest-tier threshold represented in this case. It is also the Threshold with the highest number of PRIs.

Table 3. Case 1: Example of Reportable Threshold 5-Behavioral Considerations

Observed PRIs	Associated Reportable Threshold	Tier Level	Concern Level
Demotion	None	1	Very Low
Threatening Behavior	1 – Serious Threat	2	Low
Aggression/Verbal Abuse	5 – Behavioral Considerations	3	Medium
Violence Against Person	5 – Behavioral Considerations	3	Medium

In Case 2 (Table 4), five PRIs are observed, falling into four Reportable Thresholds. One PRI, *not following procedures*, is associated with Threshold 4-Personal Conduct at Tier 2 (Low concern); express ill-will towards U.S. is associated with Threshold 2-Allegiance at Tier 3 (Medium concern); two PRIs (*compliance violation, introduction of unauthorized software*) are in Reportable Threshold 10-Misuse, which is at Tier 4 (High concern); and *enabling/facilitating foreign agent* is in Threshold 3-Espionage, which is at Tier 5

(Very High concern). If we adopt a reporting rule that selects the Threshold with the highest representation, Threshold 10-Misuse would be reported. On the other hand, if we choose to report the highest-concern Threshold represented in the case, we would report Threshold 3-Espionage.

It is possible, of course, that ambiguous situations can occur where there are multiple occurrences of Thresholds within the highest Tier—such as observing a case with PRIs in Threshold 6-Criminal Conduct and in Threshold 11-Terrorism. In such cases, analysts may use their expert judgments to select the most appropriate Reportable Threshold. It is also possible to develop automated decision support by computing risk scores that take additional factors into account, such as the severity values of individual PRIs comprising the case.

Table 4. Case 2: Example of Reportable Threshold 3-Espionage

Observed PRIs	Associated Reportable Threshold	Tier Level	Concern Level
Not Following Procedures	4 – Personal Conduct	2	Low
Express Ill-Will Towards U.S.	2 – Allegiance	3	Medium
Compliance Violation	10 – Misuse	4	High
Introduction of Unauthorized Software	10 – Misuse	4	High
Enabling/Facilitating Foreign Agent	3 – Espionage	5	Very High

The bottom-up approach will also facilitate data gathering at a greater granularity than the thirteen thresholds: There are important lower-level sub-classes of the Reportable Threshold taxonomy that are of interest to stakeholders—such as sexual assaults, fraud/financial crimes, domestic violence, etc. – these sub=classes are identified as ovals in Figure 3. For example, a stakeholder may request a report on the number of sexual assault cases in a month. Sexual assaults are in the Criminal Conduct threshold (Threshold 6), but a simple enumeration of Threshold 6 cases does not answer the request. Only those cases that meet the *criterion* (i.e., that they involve sexual assault, in this example) should be counted. An expedient way to answer this type of request is to count only those cases that contain a PRI that meets the criterion. Thus, a bottom-up method based on PRIs is as follows (using the criterion, Sexual Assault, as an example):

- For every CASE that has been designated to be associated with Threshold 6 (Criminal Conduct), identify all *observed* PRIs.
- For every such PRI connected to the case, determine if the PRI meets the criterion (in this example, it must be related to sexual assault).
- If at least one observed PRI in any CASE meets the criterion, then count this case.

This should provide a count of the number of cases that fit the criterion. This approach allows the analyst to account for details of interest within a threshold—such as sexual assaults—that would otherwise be “lost” in the general category of Criminal Conduct. This is also illustrated in Figure 4, which depicts the network

of associations (or patterns) that distinguish criminal conduct sub-classes. Implementing the knowledge base framework at this level of granularity will enable more detailed analysis and reporting by the Hub analysts. Note, also, that the link between a case and applicable Threshold (or threshold sub-class) can be recorded at the time the case is resolved/reported. In this way, statistics and other details about specific types of cases will later be immediately available, thus saving labor hours that would otherwise have to be expended in developing post-hoc reports to stakeholders/management.

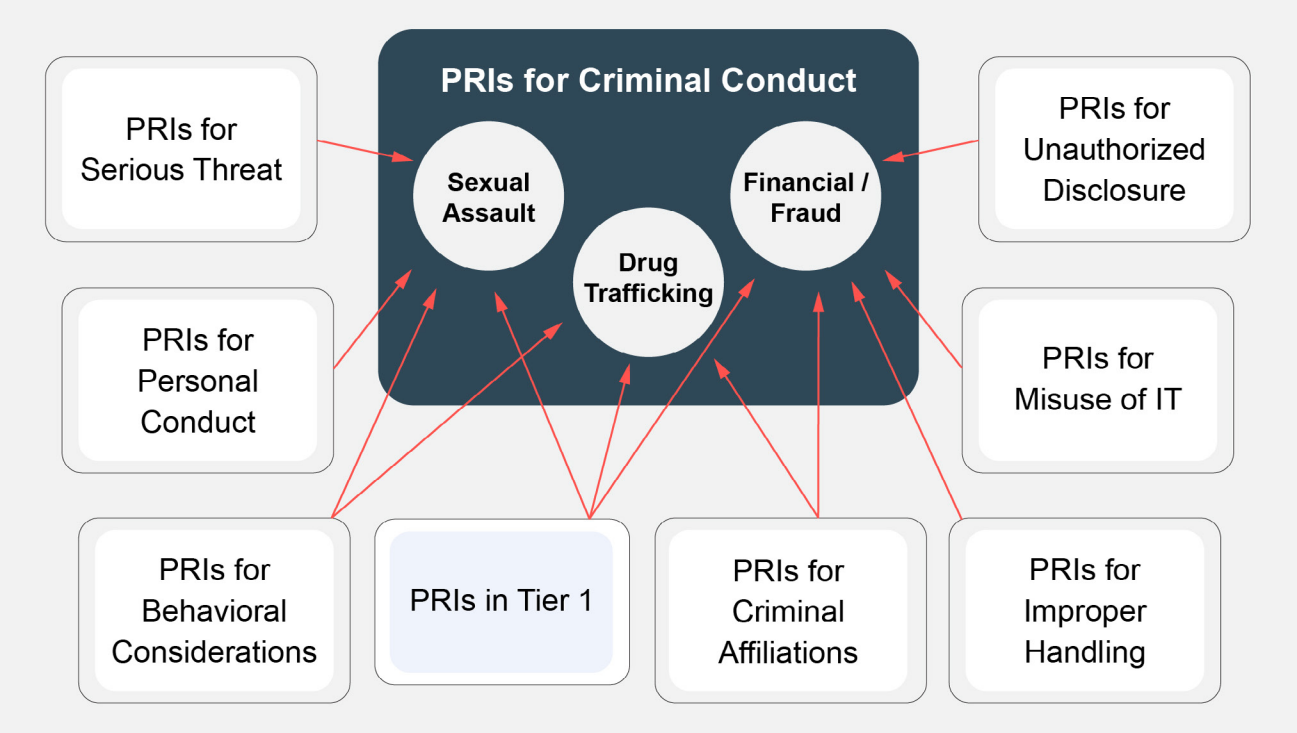


Figure 4. Hierarchical Associations Within Criminal Conduct Threshold Sub-Classes

Conclusions and Recommendations

The Threshold taxonomy, including additional sub-classes as appropriate within the 13 Reportable Thresholds, can be applied to help align current analytic processes employed by various threat assessment tools – including Cogynt – with DoD reporting requirements. Further work is needed to define these patterns at a higher level of abstraction (as conceptualized in Figures 3 and 4) and integrate this framework into a working model. Current knowledge bases (such as SOFIT) and advanced hierarchical threat models (such as Cogynt) that seek to meet best practice standards already employ multiple, rich hierarchies (taxonomies) such as the PRI class structure itself (e.g., [1]), a set of threat behavior types (e.g., [5]), and a classification of Critical Pathway-inspired PRI "role types" [1][3]. The role-type taxonomy has proven useful

in understanding possible decay characteristics of PRIs [3] [6]. Adding a Reportable Thresholds taxonomy to this set of hierarchical structures (depicted in Figure 5) can not only improve efficiency of reporting as argued above, but it also can enhance predictive analytics through pattern-based processing.

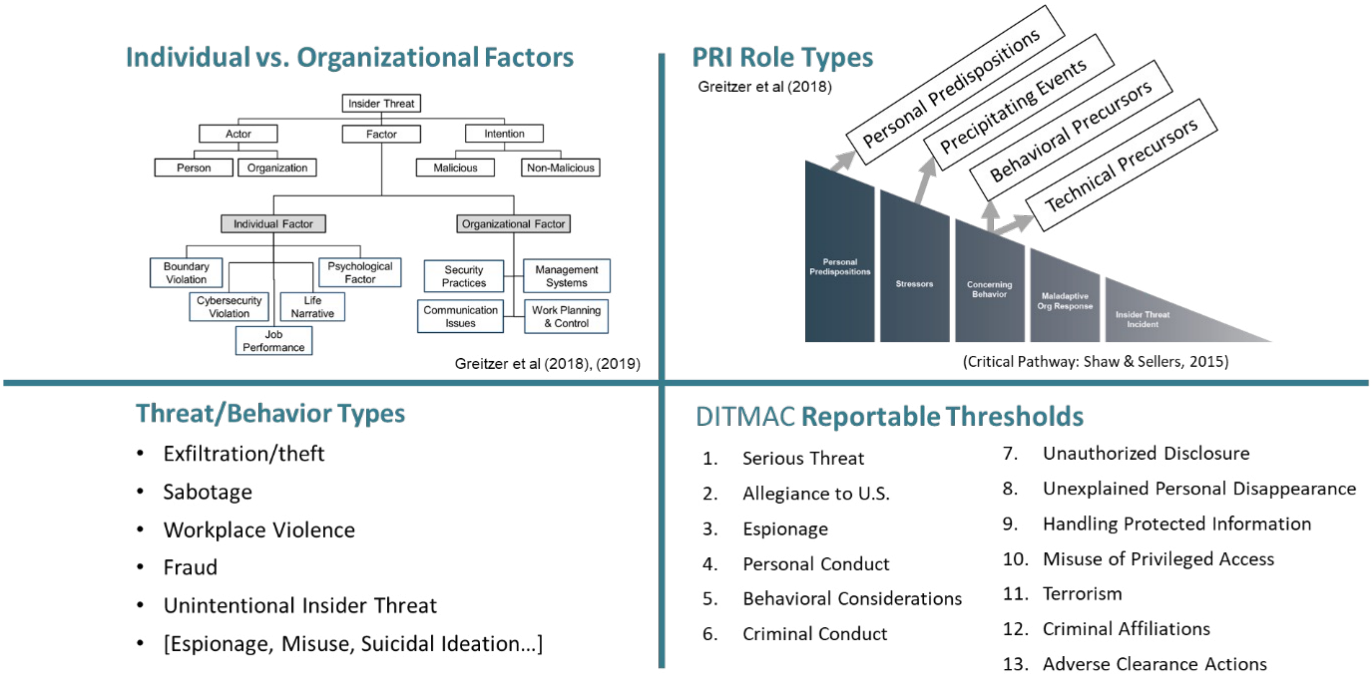


Figure 5. Multiple Classification Structures for Insider Threat PRI Knowledge Base

A pattern-based computational framework that is more sensitive to combinations of – or interactions between – PRIs may be fruitful in modeling expert judgments of insider risk. Current research suggests that assuming the contributions of PRIs to insider risk are independent may limit the effectiveness or accuracy of insider threat models [3]. Thus, by examining patterns of PRIs that discriminate between Threat/Behavior Types (or Reportable Thresholds), we can make finer distinctions between similar threat behaviors. For example, Terrorism and Espionage share several characteristics (such as associations with foreign adversaries or extremist groups) that make them more difficult to distinguish, but a pattern-based threat assessment approach can also take distinguishing features into account—i.e., since spies will tend to "stay below the radar," they may not exhibit typical concerning behaviors (e.g., Personal Conduct or Criminal Conduct concerns) that would otherwise be more likely to be identified in terrorist behavior. Similarly, the association of Behavioral Considerations with Workplace Violence (especially psychological or psychosocial PRIs) can help a pattern-based threat assessment approach discriminate between Workplace Violence and Terrorism.

While the present examination of the 13 reportable thresholds was not intended to identify new Cogynt patterns at higher levels of abstraction, this conceptual study suggests that extending the patterns

defined to date for the Cogynt DAF C-InTP model to incorporate higher-level structures (such as the Reporting Threshold hierarchy) may prove useful. Just as the implementation of hierarchical, pattern processing at lower levels of the framework (such as the Lexicon-to-PRI mapping) facilitates identification of PRIs observed in a case, the incorporation of patterns at higher levels of abstraction can inform threat assessment processes that are more sensitive to the influence of *combinations* of PRIs and their interactions. Unlike the typical computational approach employed by threat assessment models that (conveniently, but not accurately) assume PRIs act independently, the recommended hierarchical/pattern-based approach employing HCEP at higher levels of abstraction promises to produce threat assessments that better match expert judgments. The multi-tiered conceptual framework for Reportable Thresholds described here—and other hierarchical structures more generally—merit further study to support development of these more sophisticated insider threat models.

References

[1] Greitzer, FL, J Purl, YM Leong, & DE (Sunny) Becker. (2018). SOFIT: Sociotechnical and Organizational Factors for Insider Threat. In *2018 IEEE Security and Privacy Workshops*, San Francisco, CA, May 24, 2018.

[2] Greitzer, FL, J Purl, PJ Sticha, MC Yu, & J Lee. (2021). Use of Expert Judgments to Inform Bayesian Models of Insider Threat Risk. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 12(2), 3-47. June 2021*. DOI:10.22667/JOWUA.2021.06.30.003 https://dx.doi.org/10.22667/JOWUA.2021.06.30.003. Supplementary files available at: http://isyou.info/jowua/abstracts/jowua-v12n2-1.htm

[3] Greitzer, FL, & J Purl. (2022). The dynamic nature of insider threat indicators. S*pringer Nature Computer Science*, 3(102). https://doi.org/10.1007/s42979-021-00990-1.

[4] Shaw, ED & L Sellers. (2015). Application of the critical-path method to evaluate insider threats. *Studies in Intelligence*, 59(2), 1-8. https://cyberwar.nl/d/fromCryptome/cia-cpm-insider-risks.pdf

[5] Intelligence and National Security Alliance (INSA). (2021). Categories of Insider Threats. White Paper, available online: https://www.insaonline.org/docs/default-source/default-document-library/2022-white-papers/insa-wp-categories-of-insider-threats-1.pdf

[6] Greitzer, FL, RA Kliner & S Chan. (2022). Temporal Effects of Contributing Factors in Insider Risk Assessment: Insider Threat Indicator Decay Characteristics. Paper presented at *ACSAC Conference Workshop on Research for Insider Threat (WRIT)*, Austin, TX, December 2022.