Building a UAM Triage Process That Holds Up to DCSA Review

User activity monitoring produces alerts. An insider threat program is judged on what it does with them. This paper lays out seven elements of a triage process that is consistent, documented, and easy to show a reviewer, for Department of War (DoD) components and cleared contractors alike.

Why triage is where programs succeed or stall

Most programs can turn on monitoring. Fewer can explain, alert by alert, why an analyst closed one event and referred another. That explanation is what leadership, legal counsel, and oversight reviewers ask for, and it is what protects both the mission and the workforce being monitored.

For cleared industry, 32 CFR Part 117 (NISPOM) §117.7(d) requires an insider threat program that gathers, integrates, and reports relevant and available information indicative of a potential or actual insider threat. DCSA's Industrial Security Letter (ISL) 2026-01, issued May 20, 2026, consolidates the minimum standards and states that DCSA will assess compliance as part of the contractor's annual self-inspection. A documented triage process is the clearest evidence that the “gather, integrate, and report” requirement is actually happening.

What ISL 2026-01 emphasizes

- Written insider threat procedures (§117.7(b)(4))
- An Insider Threat Program Senior Official (ITPSO), appointed in writing
- The FSO as an integral member of the program team
- Gathering, integrating, and reporting relevant indicators, including SEAD 3 and SEAD 4 reporting
- Program personnel and workforce training (§117.12(g))
- Program compliance included in the annual self-inspection

Seven elements of a defensible triage process

1. A written triage procedure tied to the insider threat plan

Write down how alerts arrive, who reviews them, what each disposition means, and when an event moves to the hub or a referral. Reference it from the insider threat plan so a reviewer can trace policy to practice.

2. Severity tiers with time standards you set and meet

Define tiers by potential harm, not by tool category, and set a review time standard for each. Choose standards the team can actually hold; then measure against them. A missed standard that is documented and explained is stronger evidence than an unrealistic one.

3. A recorded disposition and rationale for every alert

Every alert should end in a defined state, such as closed with no concern, closed as a policy or training issue, held for more information, or referred, with a short written rationale. Undocumented closures are the most

common gap a reviewer will find.

4. Context from outside the monitoring tool

An alert alone rarely tells the story. Triage should pull in authorized context from security, human resources, counterintelligence, and IT, such as role changes, reportable events, and access history, so analysts are integrating information rather than reacting to a single data point.

5. A consistent decision method

Two analysts looking at the same facts should reach the same outcome. TMPC uses its 8-Step Insider Threat Decision Process® so each decision follows the same questions and leaves the same record, which makes outcomes defensible and repeatable.

6. Oversight of the people doing the monitoring

Monitoring analysts and privileged users hold significant access themselves. Audit analyst queries, separate duties, and involve legal and privacy reviewers in procedures. TMPC's Watch the Watcher® framework applies that oversight to privileged users and to the program itself.

7. Metrics that feed leadership and the self-inspection

Track alert volume by tier, time to disposition, referrals, and recurring causes such as training or configuration issues. Report them to leadership on a regular rhythm; TMPC uses PowerPoint Quad® reporting for a one-look summary. The same records become the evidence package for the annual self-inspection.

Self-check before your next review

	Question	Evidence a reviewer may ask for
☐	Is the triage procedure written and referenced in the insider threat plan?	Plan and procedure, with version dates
☐	Does every alert end in a defined disposition with a rationale?	Sample of closed alerts and their notes
☐	Are severity tiers and time standards defined and measured?	Tier definitions; time-to-disposition report
☐	Do analysts integrate security, HR, CI, and IT context?	Case files showing sources consulted
☐	Is analyst and privileged-user activity itself audited?	Audit logs and oversight review records
☐	Are program personnel and the workforce trained per §117.12(g)?	Training completion records
☐	Is the program included in the annual self-inspection?	Self-inspection report and corrective actions

How TMPC helps

Our team brings more than 30 years of combined insider threat experience and the proprietary processes built from it. For 8 years, TMPC has delivered continuous counter-insider threat and user activity monitoring support to a DoW (DoD) customer, work that drove that program to a #1 ranking among 24 DoW components by DCSA and DIA.

To talk with our team, contact info@tmpcinc.com or 813.524.6935.

References

1. 32 CFR Part 117, National Industrial Security Program Operating Manual (NISPOM), §117.7 and §117.12. ecfr.gov
2. DCSA, Industrial Security Letter ISL 2026-01, Insider Threat Program Minimum Standards, May 20, 2026. pclt.defense.gov
3. Executive Order 13587 and the Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.
4. Security Executive Agent Directives (SEAD) 3 and 4.
