ATARC

ATARC'S INSIDER RISK WORKING GROUP

Insider Risk 2025 Update

From Quiet Concern to Strategic Priority

powered by GovExec

The Insider Risk Working Group met to discuss the evolving landscape of insider risk management within Federal agencies, the supporting defense industrial base (DIB) and commercial organizations . The discussion explored the shift from reactive to proactive strategies, an increasing recognition of human factors discoverable within the organization and to the growing use of external data signals, plus the challenges of information sharing within the government circles, DIB and commercial organizations.

Evolving Approaches to Insider Threat

The discussion highlighted a significant shift in how agencies approach insider threats. Over just a few years, the perception has evolved from viewing these threats solely as counterintelligence or cybersecurity issues to recognizing their roots in the complexities of human behavior. To enable this shift is the need for expanded data sets, technologies, policies and processes.

As such, organizations now emphasize evaluating context, drawing insights from multiple internal and external data and information layers instead of singular cybersecurity data points. By linking seemingly minor incidents, stressors, relationships and concerning behaviors, organizations can discover and correlate early risk signals to better articulate concerns and develop proactive solutions that are appropriately tailored to the situation and individuals involved.

Participants also acknowledged the scope of insider risk is broadening. Instead of focusing on just cleared populations, organizations now consider all potential sources of insider risk, including contractors and research partners who have either cyber and/or physical access– not just from employees.

> **“Human phenomena aren’t predictable, not 100%. So we approximate, we give best judgments, and we lean a lot into research.”**

Importance of Human Factors

Members emphasized a growing recognition of the human factor in mitigating insider threats. The working group agrees insider threat is a human phenomenon requiring a multi-disciplinary approach.

A shift from a reactive to proactive approach enables organizations to not only mitigate risk earlier but can also yield significant positive outcomes for currently high-risk individuals who would benefit from early support. This will also enable more retention of employees moving down the pathway versus adjudicating employees after it's too late.

> **"Think holistically across your organization. In some cases, these risk signals, if discovered early, can have really positive outcomes."**

Several working group members highlighted a correlation between risk signals for insider threat and those associated with violence and suicide. One participant shared that their agency prevented several suicides by adopting holistic insider risk approach focused on identifying human-centered data signals.

For controls that cannot be automated—such as contingency plans, incident response procedures, or training records—the standard still applies: they must support operational execution, not just compliance. These plans always need to exist, but not all plans should look the same. A complex on-premise system may require a detailed continuity and recovery strategy. A SaaS application with no local dependencies might require little more than a notification chain and vendor escalation procedure. One plan might span a few dozen pages; another might fit on an index card. The difference should reflect operational reality—not control interpretation. Plans should be actionable, tailored to mission context, and tested periodically through drills or incident simulation. Their purpose is to guide real-world response—not to satisfy auditors. If a plan doesn't inform decision-making during an outage, it needs to be rewritten—not expanded. These controls are validated through execution and ownership—not word count.

Technology and Information Sharing

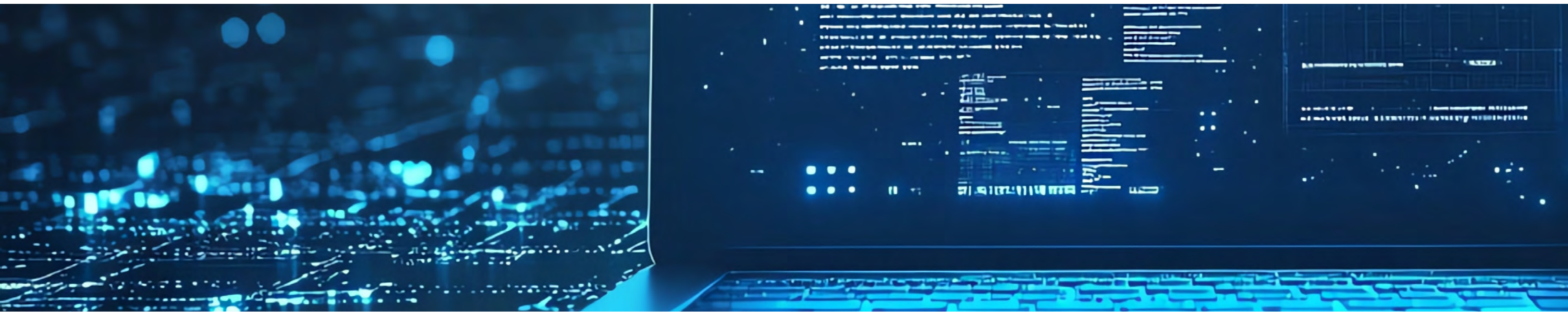
Organizations are increasingly leveraging technology to enhance monitoring and early detection of insider risk. Many are working to build integrated data systems that would enable better visibility into where information gaps exist. One participant highlighted the potential of using AI to continuously monitor People of Concern (POC) for specific signals across various platforms, and data sets.

While significant challenges to external information sharing persist, some organizations are making improvements to internal information sharing and communication. For instance, some are establishing limited information pipelines between specific departments, such as personnel security, to obtain more contextual information about individuals.

> **"Trying to pinpoint and stay left of any kind of incident is very difficult. There's only so much a human can actually do. We are reliant on the advancement of technical tools."**

However, barriers to information sharing remain a significant challenge to effective insider threat management. Many organizations rely on information from other sources to enrich comprehensive risk profiles. A centralized or integrated data system would help agencies track and identify high-risk individuals moving from one agency to another.

Sharing insider risk information with other agencies is critically important for prevention, but is often not possible due to legal constraints, privacy concerns, and lack of formalized processes. Participants emphasized a notable difference in how the DOD and civilian agencies approach insider threats, pointing to civilian privacy protections that do not pertain to military personnel.



> **“Culturally, we think there’s a semblance of privacy when we log on to a government computer in the FedCiv space. It’s even to a point where we can’t get policy in place to allow FedCivs to actually identify insider threats.”**

Civilian agencies face significant constraints regarding the sharing of information about POCs. Balancing the need to protect individual privacy rights with the imperative of addressing potential risks requires careful consideration. While participants recognized the importance of upholding privacy laws, many agreed that policy amendments are needed to facilitate more robust insider risk management.

In the absence of broader policy changes, agencies are proactively developing their own governance models and collaborating closely with legal and ethical advisors. Some have successfully integrated privacy into their organizational culture, policies, technology and operations, prioritizing the acquisition of information through the least intrusive means possible when investigating allegations.

> **“We bake in our privacy right from the beginning.”**

In addition to these approaches, other organizations employ nondisclosure agreements to restrict access to information to only those with a legitimate need. Some participants are working to educate legal teams, noting challenges with their levels of understanding insider risk. Another member shared their approach of “flattening” the organization’s hierarchy to facilitate open discussions about risk, sometimes even involving the individual in question directly.

Across the board, it was agreed that each situation necessitates a thorough evaluation to determine an agency’s “duty to warn” and to decide what information can be shared, with whom, and when. It was noted that the maturity of insider threat programs varies significantly between organizations, which subsequently affects how insider threat management is perceived and implemented across the enterprise. Ultimately, the working group agrees that more education about how to deter, detect and mitigate insider threats is needed.

Final Thoughts

In this roundtable discussion, participants underscored the growing urgency and complexity of insider risk management in today's dynamic threat landscape. The shift to hybrid work, the spread of disinformation, rising mental health stressors, and increasingly sophisticated adversaries have transformed insider threats into a multidisciplinary challenge—requiring a careful balance between unpredictable human behavior, evolving privacy laws, and organizational security.

Agencies are working diligently to detect insider risks early, prevent incidents, and collaborate across sectors when possible. As the field evolves beyond traditional enforcement models, it is cultivating a distinct and diverse professional community committed to innovation and ethical risk management.

To effectively navigate this landscape, a collaborative and integrated approach—combining technology, human insights, and forward-looking policy—will be essential to strengthening the federal ecosystem's ability to proactively address insider threats while preserving public trust and institutional integrity.