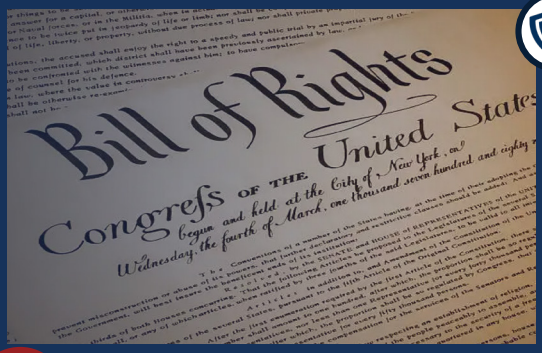
BTAC BULLETIN

BEHAVIORAL SCIENCE | LAW ENFORCEMENT & COUNTERINTELLIGENCE | CYBERSECURITY | EMPLOYEE MANAGEMENT RELATIONS | THREAT ASSESSMENT & MANAGEMENT

PROTECTED SPEECH AND INSIDER THREAT

The First Amendment to the United States Constitution protects freedoms of speech, religion, the press, and assembly. Insider threat programs cannot monitor individuals solely because they engage in protected activity. However, the content of protected speech may be relevant to a potential insider threat when combined with other behavioral and contextual indicators. The speech itself is not typically a threat; rather, it can provide, when examined with other behavior, context that indicates an employee is moving toward a malicious act. Protected First Amendment words or actions may cross the line indicating insider threat risk when the isolated expressions are accompanied by other demonstrable, objective, pre-defined behavioral risk indicators. Insider threat programs must focus on the conduct as a whole and the potential for harm, not just the speech in isolation. Insider threat programs should consult with their legal counsel when in doubt if the speech or conduct is proteted.



Protected Expression	Risk Indicators	Potential Insider Threat
Voicing strong controversial political or ideological beliefs.	Combined with unauthorized network access, unreported foreign contacts, or sudden unexplained wealth.	Unauthorized Disclosure, Sabotage, Malicious Data Exfiltration, Espionage.
Venting deep frustration about supervisors, agency policies, or coworkers.	Escalation into severe workplace disruption, repeated physical security violations, or aggressive posturing.	Workplace Violence, Sabotage.
Discussing or researching historical events of treason, leaks, or violence.	Paired with attempts to bypass IT security protocols, sudden performance drops, or unauthorized data downloads.	Malicious Data Exfiltration, Workplace Violence, Espionage.

Insider Threat Program – Holistic Assessment

To contextualize protected speech, insider threat programs should follow a deliberate, fact-specific, and legally guided process that integrates objective data from other domains (i.e. physical security, cybersecurity, HR). Indicators such as unauthorized data access, abnormal work hours, or bypassing security controls transform potential risk from protected speech into actionable insider threat information.

- **Analyze Content:** Assess the statement. Is it specific, detailed, targeted?
- **Analyze Context:** Are other objective anomalies or risk indicators present? Evaluate speech, not in isolation, but in the context of other potential indicators.
- **Legal Consultation:** Consult with legal counsel and civil liberties officers early using pre-coordinated legal boundaries to ensure the program's actions are legally defensible, respect employees' freedoms, and escalate actual threats.

EXAMPLE:

An employee voices extreme frustration about a specific organizational policy (a protected expression). On its own, it is a grievance that does not immediately warrant an insider threat response. However, if the employee's supervisor reports that cyber logs simultaneously show the same employee attempting to download gigabytes of data related to that policy onto an unauthorized thumb drive, and physical security logs show the employee accessing the building at 2 AM, the program now has a more holistic, actionable scenario of escalating insider risk.

Insider threat programs are intended to identify and assess risk before it escalates to a harmful act. When the protected speech is analyzed alongside other available data (HR records, network activity, physical security records), insider threat programs are better positioned to assess if the individual poses a potential threat that requires mitigation. This approach ensures that civil liberties are respected, but the subsequent unauthorized actions are mitigated before harmful acts occur.

Overreach

An insider threat program overreaches and potentially infringes on free speech or freedom of expression when it targets an individual for beliefs or protected speech itself, rather than for conduct that indicates a threat. Overreach occurs when insider threat programs:

- Monitor an employee simply because the employee attended a political rally, donated to a lawful advocacy group, or expressed political or religious views when there is no other behavior indicating a threat.
- Target individuals: For example, create UAM triggers to target employees based on personal characteristics, political affiliation or religious beliefs, rather than on pre-defined, neutral behavioral indicators.
- Establish excessively broad data collection not rationally related to identifying legitimate insider threats.
- Exercise 'Thought Policing': For example, open inquiry on employee for criticizing agency policy.
- Ignore Context: Treat every mention of violence as an actual threat without considering the context, intent, specificity (i.e. crude joke, quote from movie, angry venting, political hyperbole/commentary).
- Lack Legal Guidance: Make determinations without consulting agency legal counsel or civil liberties officers.

A sound insider threat program is behavior-focused and threat-based. Programs overreach the moment they become belief-focused and content-based in a way that punishes protected expression.