When Trust Erodes, Why Security Clearances Still Matter

by Brett Mencin
President,
Enterprise Vetting & Analysis

XCELERATE

Two recent national security incidents, although they seem very different on the surface, share a common thread: the misuse of trusted access.
In one case, a U.S. Army Special Forces soldier allegedly used classified operational knowledge to place bets on a geopolitical event, resulting in a hefty profit of more than $400,000. [1]

In another case, a former Army employee was charged with leaking classified information to a journalist, exposing sensitive national security material to unauthorized channels.[2]
These are not just isolated lapses in judgment. They are warnings.

The Expanding Insider Threat Landscape
Insider threats were often seen as espionage agents in the shadows, covertly passing secrets to foreign enemies, cloak-and-dagger actions straight out of a James Bond movie. Today, people's motivations are more diverse, intricate, complicated, and sometimes even technology-enabled. It can be as simple as needing extra cash or as simple as poor judgment. In the current political environment, it can also be to take a stand, feed an ego, or respond to external pressures.

The alleged betting scheme tied to the Venezuela operation is a valuable case study. Prosecutors say the individual leveraged advance knowledge of a planned U.S. military action (information entrusted to him because of his clearance) to exploit a modern digital marketplace.[3]

This is a 21st-century insider threat: not a spy in a trench coat, but a cleared professional using emerging platforms to monetize privileged information.

Trust Is Not a Checkbox
Security clearances are often misunderstood as a one-time vetting hurdle. In reality, they represent an ongoing contract between the individual and our nation.
Access to classified information is not a right. It is a condition of trust.
That trust must be continuously validated.

The second case alleged unauthorized disclosure to a journalist. This isn't new, but a reminder that as motivations vary, so must prevention strategies. Here, the issue isn't financial exploitation but a breakdown in judgment, adherence to protocol, and respect for classification boundaries by someone attempting to take a stand.
Different motivations, same root issue: trusted access without ongoing accountability.

What This Means for Agencies and Contractors
For organizations in national security, these events underscore the importance of three main actions: continuous vetting, connecting diverse data sources, and building an accountable culture.

Periodic reinvestigations are no longer sufficient. Behavioral signals, financial anomalies, digital activity, and foreign contacts must be monitored in near real-time, where legally permissible. Connecting the dots across systems, including HR, security, financial disclosures, and cyber activity, is critical. Siloed data = missed warning signs. Policies alone do not prevent insider threats. A culture that reinforces accountability, ethical decision-making, and reporting concerns is just as important as technical safeguards.

The Technology Factor: New Platforms, New Risks

Prediction markets, cryptocurrency, and encrypted communications are no longer fringe tools. They are mainstream, accessible, and in some cases, lightly regulated.

In the Maduro-related case, authorities allege the use of blockchain-based platforms to place and potentially obscure transactions.[4]

That matters because it makes financial misconduct harder to detect, anonymity lowers perceived risk, and transactions happen so quickly that they can outpace oversight.

Clearance holders are operating in this same environment. Vetting and monitoring must evolve accordingly.

The Bottom Line

Security clearances are foundational to national security, but they are not fail-safe. It is essential that agencies and contractors proactively strengthen vetting and monitoring systems, foster accountable cultures, and adapt to evolving threats to ensure ongoing protection.

The recent cases are reminders that the greatest vulnerabilities are not always external…they often sit behind the firewall, badge in hand, fully trusted.

About the Author

Brett Mencin, President of Enterprise Vetting and Analysis, oversees all associated contracts, supporting DHS, DCSA, U.S. Army, FBI, OMB, IC, and other federal agencies.

In addition to supporting defense clients, Brett is Xcelerate's Chief Security Officer. In this role, he has created a robust framework for implementing information security strategies, policies, and procedures. He ensures compliance with relevant regulations and manages Xcelerate's overall security risk posture.

Brett has almost 20 years of experience supporting all aspects of the Personnel Vetting mission, from reengineering processes to consolidating functions across the Federal Government. He is a recognized Subject Matter Expert and has spoken at numerous industrial security conferences.

Brett holds an MS from the University of Virginia and a BS from the University of Colorado at Boulder.

Brett Mencin
President, Enterprise Vetting & Analysis
bmencin@xceleratesolutions.com

Sources

[1] Orden, Erica, April 28, 2026, Soldier Who Placed Polymarket Bet On Maduro Operation Pleads Not Guilty, Politico Online
[2] Reilly, Grumback, and Uribe, April 8, 2026, Former Army Employee Charged with Leaking Classified Info to Journalist, NBC News, National Security
[3] Department of Justice, Press Release April 23, 2026, U.S. Soldier Charged With Using Classified Information To Profit From Prediction Market Bets
[4] Ibid.