

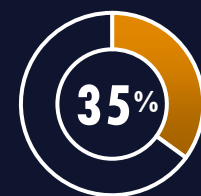


BTAC BULLETIN

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

ELICITATION INSIDER THREAT RISKS

Elicitation is a technique used by nefarious actors (e.g., *Foreign Intelligence Entities, Criminals, Corporate Competitors*) to gather information without the target's knowledge, using what appears to be normal or mundane social and professional contacts. Elicitation efforts create significant insider risk across the government and cleared industry, on the pathway to a collusive threat¹ or unauthorized disclosures (UD). While a consistent risk, opportunities for elicitation may increase during times of organizational changes and personnel transitions. These types of change can produce a landscape with potential for grievances against employers/organizations, financial difficulties, and increased social media engagement. These vulnerabilities can then be leveraged through threat vectors to acquire sensitive information that former employees or disgruntled insiders possess. It is up to every employee to **protect your clearance, reputation**, national security, and corporate standing and stay vigilant to the changing risk landscape involving the targeting of employees.



Only 35% of employees, when unambiguously approached on LinkedIn, reported the incident³.

THREAT VECTORS

- Job/Social Networking Services (SNS):** Nefarious actors may pose as employers or use data from job platforms like LinkedIn to collect and profile you for targeting/recruitment.
- Academic Collaboration:** Legitimate institutions can be used to elicit subject matter experts in sensitive fields and gain access to protected/classified information (e.g., research funding, sponsored trips, speakerships)
- Financial 'Opportunities':** During financial hardship, individuals may seek out seemingly innocuous ways to make quick money. This can be used to collect information or identify vulnerabilities to be used against someone.
- Gaming Forums:** Adversaries can establish trust through in-game chats, guild memberships, and private channels, gradually eliciting sensitive details about work roles or access.

TARGETS



Targets of Elicitation: Anyone can be a target, especially those with insider knowledge or a security clearance. Those leaving their positions and looking for work, whether voluntarily or involuntarily, can become especially easy targets to entities masquerading as financial opportunities and lucrative employment.

ELICITATION TECHNIQUES

- Subtle Questioning:** Using innocuous conversation (e.g. *at a coffee shop, in a waiting room*) and ongoing or repetitive questions to gather details about work or life including questions about professional responsibilities, clearance, or work locations/capabilities.
- Professional Requests:** Online surveys or requests for expert opinions may be used to target and leverage information.
- Exploiting Expertise:** Requests for input on special fields to develop white papers or collaborate on research appeal to ego, while probing position and accesses or gathering information on projects and capabilities.
- Flattery:** Dating services can be used for social engineering and elicitation of classified information through the public profile and use of flattery to develop emotional investment or sense of trust.

BEST PRACTICES

- Review your resume:** If you are preparing your resume for a job change, send it through organization review to ensure you are not disclosing protected/sensitive information.
- Be cautious about airing grievances:** By publicly discussing your frustrations you increase the risk of being targeted by actors seeking to elicit information or exploit your emotions to encourage disclosures of sensitive information.

- Do not answer:** Deflect, change topic, provide non-descript answers, or be blunt about limits. Legitimate job opportunities will respect classified and sensitive boundaries during job negotiations; *And always ensure you report to security or CI.*
- Opt out of data aggregators:** In all of your apps, programs, memberships there is generally a setting to request information not be shared or that your information not be scraped from the internet in tools called "aggregators".

- Secure your identity:** Be proactive about your identity security and what PII is shared on social/online platforms. Avoid posting your clearance on social/job sites which may make you a more lucrative target; Information that seems harmless individually, when aggregated, can be used for elicitation and manipulation. (*Use tools like the DoD Identity Awareness, Protection, and Management Guide and DCSA Elicitation Brochure*)



1. *Elicitation - Your Role In Keeping Our nation's Information Safe* (n.d.). The National Counterintelligence and Security Center. Retrieved 3/5/25.
 2. *Defining Insider Threats* (n.d.) Cybersecurity & Infrastructure Security Agency (CISA). Retrieved 3/5/25.
 3. Caputo, D. D., Danley, L., Doodson, J., and Bryant, D. (2020). Economic espionage: An experimental study into employee reporting of security incidents. McLean, VA: The MITRE Corporation.