# Foreign Intelligence Recruiting U.S. Gov't Employees

**(U) This infographic provides insight of Foreign Intelligence Recruitment Schemes Targeting U.S. Government Personnel.** Foreign intelligence entities are increasingly using sophisticated recruitment schemes to target current and former U.S. government employees – including those in the DoD – via social media and online job platforms. These schemes often begin with seemingly legitimate job offers from unknown recruiters offering high pay for consulting work..

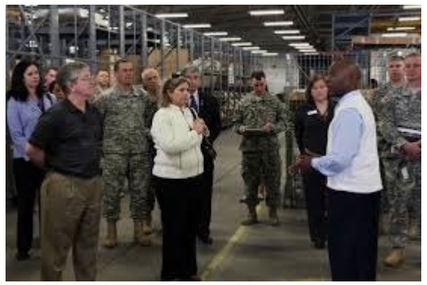
**Tactics and Recruitment Methods:** Adversaries pose as recruiters, headhunters, or representatives from legitimate companies to gain trust and extract sensitive information. They utilize platforms such as LinkedIn, TikTok, RedNote, and Reddit, and may even create fake recruitment websites. Typically, they target individuals who indicate they are "open to work."

**Objective:** Their goal is to collect sensitive information, including unclassified data, that could provide a strategic advantage. They often aim to build relationships rather than immediately seeking classified secrets.

**Red Flags:** Signs to watch for include unusually high compensation offers, pressure to communicate outside of secure platforms, use of encrypted messaging, urgency in demands, and requests for detailed information. This situation reinforces longstanding concerns that mass layoffs could create opportunities for foreign intelligence services to recruit personnel.

LinkedIn Rednote Tik Tok reddit

**Target Audience:** Anyone with a background in the U.S. government is a potential target, including active-duty personnel, reservists, civilians, contractors, and retirees. Disgruntled and financially vulnerable former employees are particularly seen as easy targets for providing valuable insights regarding U.S. infrastructure and government operations. Recently fired employees with security clearances and probationary employees are especially susceptible to these tactics.



**Reporting :** Self-reporting is crucial as the scale of this threat is too large to investigate solely through official channels. Vigilance and awareness are vital for force protection in the digital age. This is a long-term social engineering campaign designed to appear professional and legitimate, exploiting personal freedoms and blurring the lines between counterintelligence and force protection.

FBI Federal Bureau of Investigation


Click images to go to reporting site

This long-term social engineering campaign is crafted to seem professional and exploits personal freedoms while blurring the lines between counterintelligence and force protection. Experts warn that this poses a serious national security threat with real-world consequences. The risk of exploitation grows due to job insecurity, lack of institutional knowledge, and foreign recruitment efforts.

**Source:** Foreign intel job scams target current, former DoD employees **(Space Force)**; Exclusive: US intel shows Russia and China are attempting to recruit disgruntled federal employees, sources say **(CNN)**