

The Alert Resolution Gap in Continuous Vetting

What DCSA Delivers, What the Facility Security Officer Still Owns, and the Window in Between

Industry's concern with continuous vetting is not the model itself. It is what happens after an alert fires. Federal News Network reported in September 2026 that cleared contractors are pressing the Defense Counterintelligence and Security Agency (DCSA) for better metrics on how many alerts continuous vetting generates, how long they take to resolve, and what companies should do while an alert remains open.

Roughly 948,000 industry employees are enrolled in DCSA continuous vetting, about a quarter of the enrolled population. DCSA's continuous vetting framework draws from seven categories of information: criminal activity, terrorism, foreign travel, suspicious financial activity, credit, public records, and eligibility. DCSA assesses alerts to determine whether they are valid and warrant further action. For the companies that employ these individuals, an unresolved alert can represent an unquantified risk, with limited visibility into how long resolution may take or what the ultimate outcome will be.

Volume Is the Constraint

The volumes explain the concern. DOE reported 502,385 continuous evaluation alerts in one quarter across nearly 121,000 cleared individuals, roughly four alerts per enrollee. DOE expects its workload to fall when it transitions to DCSA, which will triage and validate alerts before passing actionable information to the department.

DHS processed more than 500,000 alerts in its most recent quarter, averaging 13 days to adjudicate. While 92 percent were classified as low risk, 6 percent were medium and 2 percent high, leaving roughly 40,000 alerts requiring greater attention.

The challenge is not detecting more. It is quickly separating what matters from what does not.

The FSO Owns the Risk and Is Last to Know

Industry's second request was that DCSA route alert resolution through Facility Security Officers (FSOs) rather than relying first on direct contact with the clearance holder. DCSA has acknowledged difficulty reaching some individuals who generate alerts. The request is sound. That it has to be made at all highlights a larger issue.

Under the National Industrial Security Program, the contractor owns the security risk, with the FSO designated to manage the security program. If alert information goes first to the employee, the company responsible for managing the risk may be the last to know. The consequences still fall on the contractor. As a ManTech representative put it, an open case can mean "all bets are off" on position transitions, affecting staffing, access, assignments, and contract performance while the company has limited visibility into the concern or when it will be resolved. **The takeaway:** continuous vetting depends on valid information reaching the organization that owns the risk in time to act.

Closing the Open-Alert Window

Continuous vetting answers a government question: **does this person remain eligible for access to classified information?** The contractor must answer a different one: **is something changing that could create risk, and what should the company do about it while the government process runs its course?** ClearForce Resolve™ is built to help answer the second question and complement the first.

-  **A company-owned risk picture:** Resolve™ continuously monitors relevant criminal, financial, and dual employment events across defined cleared and uncleared populations. It can combine external risk indicators with internal incident information, providing visibility into relevant changes without waiting solely on a government notification.
-  **Defensible interim decisions:** Alerts enter a documented review and case management process designed to support applicable FCRA and EEOC requirements. This gives security and other authorized stakeholders a documented basis to assess appropriate access, assignment, investigative, or other risk mitigation actions while a government matter remains unresolved.
-  **Metrics the program can report:** Detection-to-disposition timelines, alert volumes, rates per 1,000 monitored employees, and documented outcomes can give security leadership measurable insight into its own program performance and risk picture.

Continuous vetting is the right model, but eligibility is only part of the problem. **The operational gap is what happens next: Is the information valid? Does it reach the organization that owns the risk? Does it arrive in time to act? And what does the company do in the interim?** ClearForce Resolve™ helps close that gap.

Sources: [Federal News Network](#), "Contractors Want More Data on 'Continuous Vetting' Clearance Model," Sept. 2026; [DCSA, Continuous Vetting](#).