NICK DALE

A NEW ERA OF TRUST IN POLICING?

A national rollout of Continuous Integrity Screening (CIS) would mark a pivotal shift in police accountability, ensuring officers and staff uphold the highest standards of integrity.

THE SECURITY CHALLENGE: INTEGRITY GAPS IN POLICING

Public trust in policing has been shattered by high-profile cases, such as the murder of Sarah Everard by a serving police officer. These incidents have exposed systematic failures in integrity vetting processes that rely on periodic checks, leaving long gaps where integrity risks can go undetected. CIS is an evidence-based, peer-reviewed solution that enables constant integrity monitoring, ensuring misconduct is identified and addressed before it escalates.

Traditional reactive vetting in law enforcement is infrequent, often occurring only every three to ten years following an officer's initial screening. Once cleared, there is no automated mechanism to monitor their conduct until the next scheduled review. This creates significant blind spots, where officers engaging in criminal associations or unethical behaviour can operate undetected.

The current system also relies on self-reporting, expecting officers to disclose misconduct, victimisation, or criminal involvement. However, research shows that many do not—whether through fear, oversight, or deliberate concealment (a red flag and misconduct in and of itself). Without a proactive, intelligence-led approach, misconduct often only comes to light after serious incidents, by which point public trust has already been damaged. There is potential for CIS to become a deterrent.

THE SOLUTION: CONTINUOUS INTEGRITY SCREENING (CIS)

CIS is a proactive, data-driven system that continuously monitors police employees against a national intelligence database. Rather than waiting for misconduct to surface through periodic vetting or reactive investigations, CIS provides real-time screening to identify potential integrity risks, reducing the reliance on periodic vetting.

An evidence-based pilot conducted by North Yorkshire Police (NYP) screened 3,000 employees over six months, revealing:

- 18 cases were referred for further investigation, the majority linked to intelligence from other forces—previously unknown to NYP's Professional Standards Department (PSD).
- A refined system to reduce false positives, ensuring only actionable intelligence is flagged.
- The ability to enhance workforce safeguarding, identifying officers who were victims of crime and enabling welfare support.
- The pilot showed that NYP had robust vetting practices, but, also highlighted the added value of continuous screening in identifying undetected risks.

Following ongoing concerns over police misconduct and the arrest and conviction of David Carrick, this pilot study led to an 'Historic Datawash' commissioned in 2023 with over 307,000 officers, staff and volunteers checked. This datawash revealed 461 individuals were referred to an appropriate authority and of these:

- 9 triggered further criminal investigation
- 88 triggered disciplinary investigation
- 139 triggered vetting clearance
- 128 triggered management intervention
- 97 required no further action

WHY CONTINUOUS INTEGRITY SCREENING IS CRITICAL FOR SECURITY

CIS directly addresses a core security challenge: the lack of constant monitoring within policing. The ability to detect misconduct early has far-reaching implications for law enforcement and national security:

1. **Proactive risk management** – CIS identifies integrity risks before they escalate, preventing potential corruption, abuse of power, and criminal associations within police ranks.
2. **Rebuilding public trust** – transparency and accountability are central to police legitimacy. CIS demonstrates a commitment to ethical policing, reassuring the public and increasing Chief Officer confidence.
3. **Eliminating selection bias** – unlike targeted investigations, which can be reactive and inconsistent, CIS applies universal screening, ensuring fairness across all personnel.
4. **Workforce safeguarding** – the system can identify employees who are victims of crime, enabling timely welfare support.
5. **Scalability beyond Policing** – the model can be expanded nationally and applied to other sectors requiring high-security vetting, including aviation security, intelligence and civil service, where trust and integrity are critical.
6. **Leverages existing technology** – CIS integrates with existing policing systems, reducing implementation costs and reducing the need for new infrastructure and the associated costs of these.

> **While ethical concerns and resource challenges must be addressed, the benefits of real-time integrity monitoring far outweigh the limitations.**

While Continuous Integrity Screening strengthens police accountability, its implementation must be carefully managed. False positives can place extra pressure on Professional Standards Departments, requiring time and resources to investigate. Privacy concerns have also been raised, with some staff fearing the impact of continuous monitoring on morale. The system's effectiveness depends on strong data sharing between police forces—without it, critical intelligence could be missed. While CIS uses existing technology, human oversight must remain central to decision-making. These challenges don't outweigh the benefits but highlight the need for a balanced approach that strengthens security while protecting employee rights.

WHAT NEEDS TO CHANGE?

The implementation of CIS raises important ethical and legal questions, and balancing security with privacy is critical.

- **Transparency is key** – with officers and staff being informed about how CIS works, and what data is reviewed regarding flagged intelligence.
- **Strict data governance** – access to flagged information should be limited to vetted personnel within PSD to prevent misuse.
- **Proportionality and fairness** – the system should ensure that minor or irrelevant intelligence does not unfairly impact employees' careers.

Despite its success and other forces showing interest in implementing it, CIS is not yet standard practice across UK policing. Currently, NYP is the only force to have integrated CIS into its operating model. For CIS to deliver full security benefits, the following steps are needed:

- **National Implementation** – backed by appropriate regulatory bodies and law enforcement agencies by standardising CIS across all UK police forces, ensuring a consistent and intelligence-led approach to integrity screening.
- **Data-Sharing Consistency** – cross-force intelligence sharing must be strengthened, as CIS is only as effective as the data it can access.
- **Ethical Governance** – while CIS enhances security, it must be implemented with transparency and accountability to ensure data privacy and workforce trust.

Beyond policing, CIS has potential applications in other high-risk sectors. Public sector organisations, including border security, counterterrorism, aviation security and government agencies could all adopt similar models to enhance vetting, and security protocols and increase public safety.

CONCLUSION

The pilot study demonstrates that CIS is feasible and valuable in strengthening police integrity. It represents a step-change in police accountability and security. By leveraging existing available data rather than waiting for scheduled vetting, CIS closes integrity gaps, safeguards officers, and rebuilds public trust and confidence in policing. While ethical concerns and resource challenges must be addressed, the benefits of real-time integrity monitoring far outweigh the limitations.

For law enforcement to remain effective and credible, a national rollout of CIS is essential and would mark a pivotal shift in police accountability, ensuring officers and staff uphold the highest standards of professional integrity – which will quickly increase public confidence in the police service.

Expanding this evidence-based model beyond policing to other high-security sectors will further strengthen national security.

Nick Dale leads the safeguarding and policing sector in the UK for CGI one of the largest independent IT organisations in the world. He is also a PhD candidate at the University of Cambridge.

Image credit: © *JD8* | stock.adobe.com