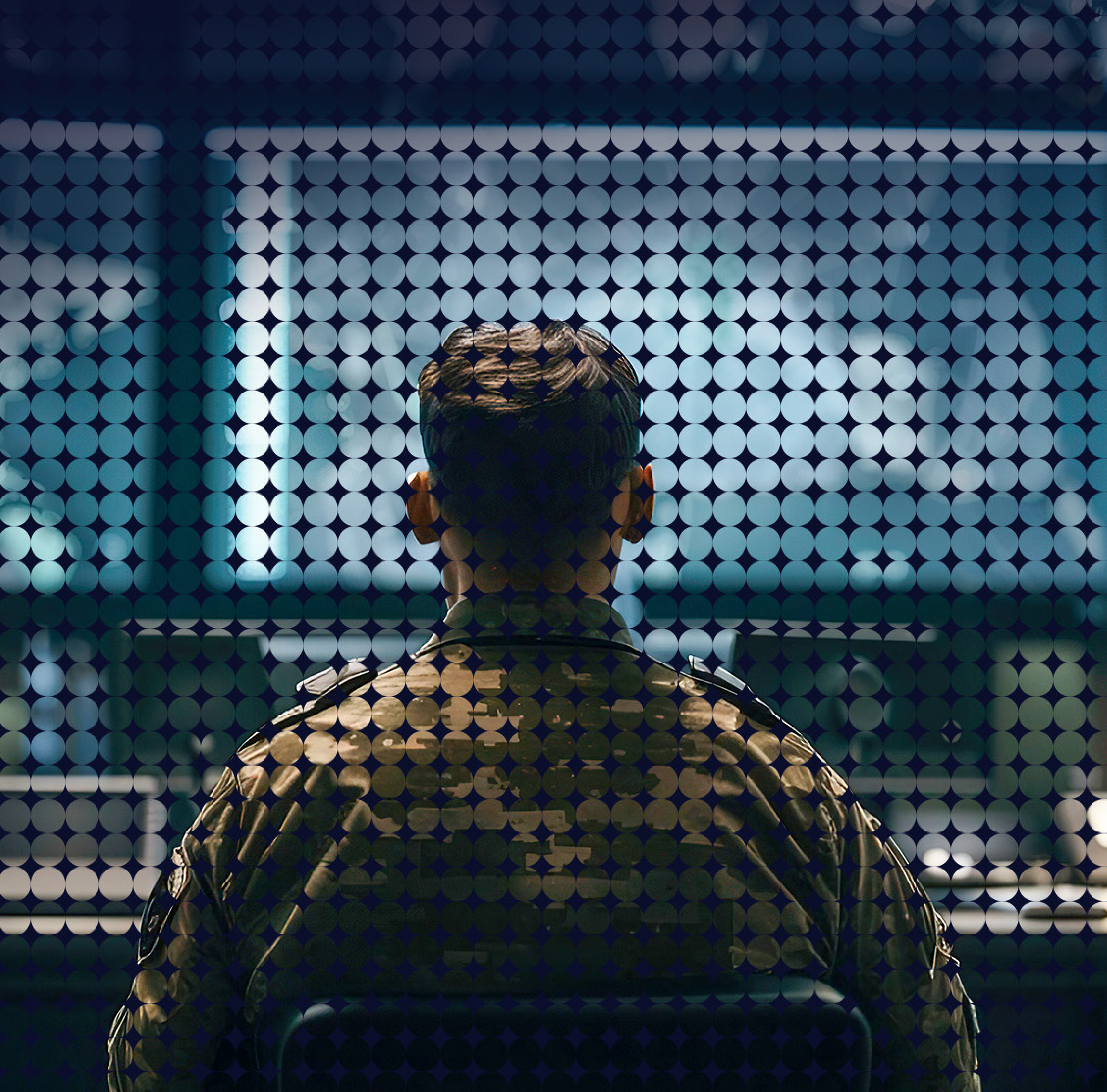
Siren
Powering investigations

SIREN PERSPECTIVE: CLOSING THE GAP

Leveraging Technology for Enhanced Quality, Accuracy and Speed in Defense Vetting

By John Randles



By John Randles

John Randles joined Siren as CEO in 2017. John has been in the Global Data Management space for over twenty years. John played a leading role in a number of well-known business success stories, as CTO of Eontec, acquired by Siebel in 2004, and as CEO of Polarlake, acquired by Bloomberg in 2012. John spent five years as CEO of Polarlake for Bloomberg after the acquisition. John has a degree in Computer Engineering from the University of Limerick in Ireland.

The imperative of robust vetting procedures for national defense forces is well-known and well-documented. In modern practice however, the gold standard has proven merely aspirational for even the most reputable institutions.

This Siren Perspective examines the current state of play in the world of vetting and the challenges posed by inadequate vetting with recent examples from defense force and law enforcement agencies around the world. It also outlines a set of recommendations for tighter controls in recruitment vetting and repeat vetting procedures aimed at reducing the risk of high profile and sometimes catastrophic abuses of power while alleviating the damaging potential of ensuing public relations fallouts.

Sub standard vetting procedures have the potential to weaken institutional integrity; undermine workplace morale and co-worker trust; can have a devastating impact on public trust in government institutions and ultimately can cost people their lives as malign individuals expose vulnerabilities to commit heinous crimes after infiltrating the very institutions designed to protect law and order and uphold national security.

As recently as December 2022, it was claimed that military leaders have no way to spot extremism on social media[1] and military background checks are limited to criminal background checks - there appears to be a knowledge gap in terms of awareness of the data and technological tools available to key decision makers. Meanwhile, the threats persist and inaction comes with a heavy price tag.

Insider attacks are very real as we have witnessed in recent times. The fear of a threat from active service members was heightened in Washington D.C. following the January 6th 2020 insurrection at the U.S. Capitol[2] and such threats are now commonplace.

This is not solely a military challenge, nor is it a US-only problem. Since 2021, in the UK alone, 16 police officers have been convicted of an offense[3]. Scratching the surface of this statistic reveals many contributing factors and known challenges for those responsible for recruiting and retaining the best police - varying political will; inadequate funding; increasingly sophisticated criminality; rapidly evolving technology; the burdensome administrative challenge of implementing robust vetting during rapid-fire recruitment drives and a cumbersome process for renewing vetting for incumbent staff.

In the wake of headline-grabbing cases detailing predatory and discriminatory behaviors within the police and other law enforcement bodies, the public outcry for 'more to be done' has an almost cyclical air of inevitability.
When such incidents occur, media outlets are quick to paint a picture - however incomplete it may be. Media reports in this domain are typically behind the times and only partially informed as investigative journalists are limited to the same out-dated methodology as laggard law enforcement agencies. They are forced to rely on data manually compiled and cobbled together often with fragile assumptions and inherent biases - a recipe for erroneous conclusions and potential litigation. Whether media reports are fully or only partially true, the PR rescue mission has already begun.

[1] https://www.military.com/daily-news/2022/12/06/military-still-has-no-good-way-spot-extremist-recruits-and-troops-social-media.html

[2] https://apnews.com/article/biden-inauguration-joe-biden-capitol-siege-ap-top-news-857bacc273e16ff82dc9fefed1242ae8

[3] https://www.express.co.uk/news/uk/1724882/sarah-everard-david-carrick-wayne-couzens-met-police-officers-convicted

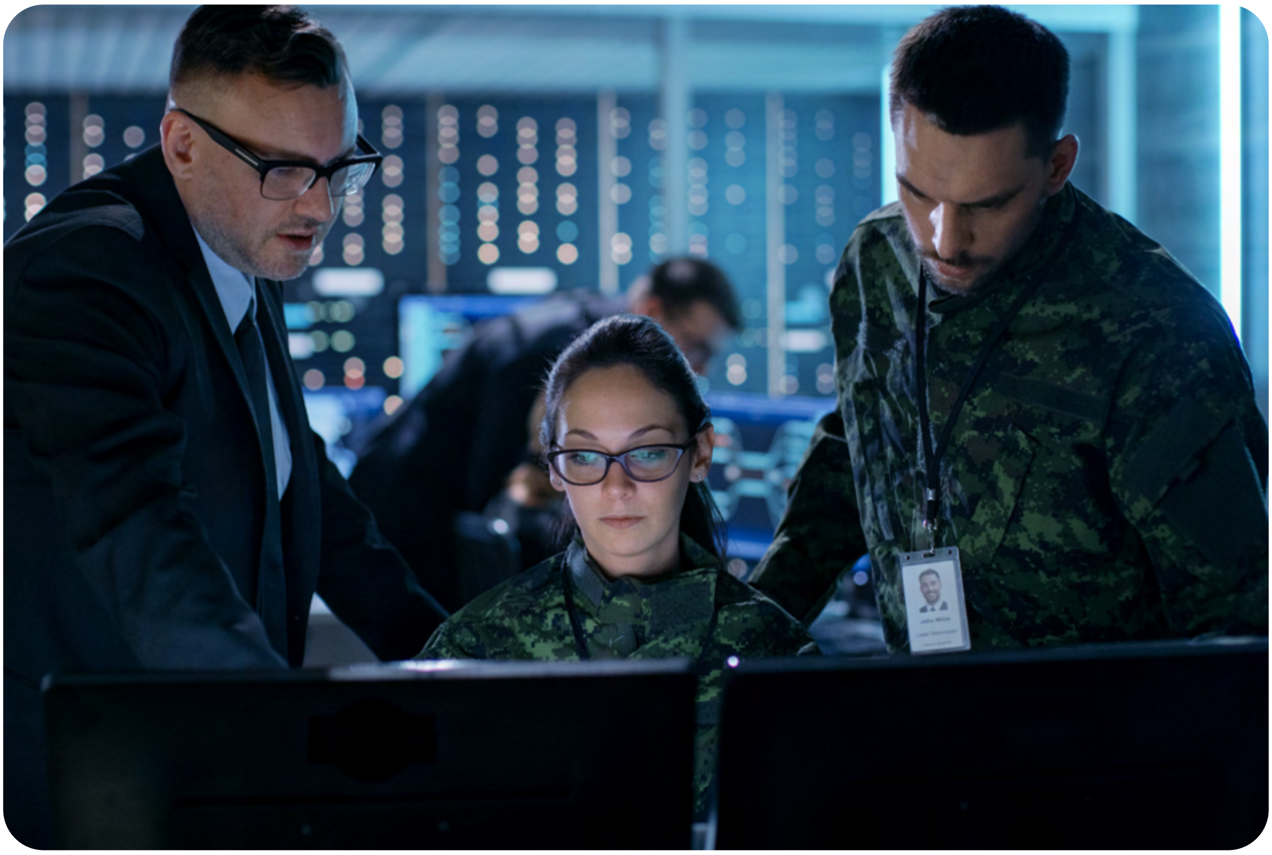
The media, like politicians, unions and the general public decry recruitment processes and hiring managers come under renewed and smothering scrutiny.

For experienced investigators in anti-corruption units, this is an all-too-familiar scenario. Over time, a fresh political scandal or climate alarm will replace these shocking headlines across tabloids and broadsheets but the challenge of rooting out internal threats within security forces remains. Such scandals also rock internal cooperation and contribute to siloed decision making.

In the modern day, the layers of threats and risks associated with hiring are manifold and when unaided by the latest technology, the likelihood for repeat headlines contribute to a slow wither of public confidence and trust in these institutions.

Hiring and maintaining a fit for purpose workforce is a difficult job but it need not be an overly burdensome administrative workload.

Thanks to Siren, the technology exists for hiring managers across national security, law enforcement and military to conduct thorough vetting in real-time and synthesize a concise and renewable report that gives them the confidence to recruit 'fit & proper' personnel.



THE RECRUITMENT CONUNDRUM

Recruitment in defence and law enforcement is rarely a continuous, linear process - in fact, it often lurches from crisis to crisis. In 2022, the US Army fell short of its recruitment goals by 25 per cent and launched a renewed recruitment drive in mid-2023[4] targeting 65,000 new soldiers. Recruiting at scale in a short time frame is a pressurized environment. Law enforcement faces similar challenges with the recent example of Australian federal police chiefs highlighting the ongoing challenge faced in recruiting and retaining police[5].

Hiring managers in the defense forces, as well as the police and corrections facilities, must respond to peaks and troughs in budgets in line with the threat of conflict and national or state economic performance. Austerity then results in recruitment freezes which, when coupled with routine retirements, places a significant strain on resources. Then as an economy recovers and unemployment levels are low, employment in the military and other security forces are a less attractive financial proposition while recruitment drives typically lag behind economic recovery resulting in waning standards of recruitment.

In the US, there is increasing concern that defense forces are susceptible to far-right political ideologies[6]. One estimated figure quoted in the New York Times suggests that more than 25% of extremist paramilitary groups have legitimate military training[7].

Reports suggest 1 in 5 officers in the US Navy have witnessed racial discrimination[8] and US Army General Mark A. Milley, who is also the US Department of Defense's Chairman of the Joint Chiefs of Staff, said most clearly in addressing discrimination: "We who wear the cloth of our nation understand that cohesion is a force multiplier. Divisiveness leads to defeat."

Vetting has a vital role to play here and automation in processing large amounts of data is a force multiplier in itself. The output of better decision-making can have a lasting, positive impact on maintaining and improving cohesion in the defense forces.

In the UK, a similar story has emerged where concern has recently been expressed at the lack of face-to-face interviews[9] in recruiting police as recruiters are forced to play a 'number's game' in response to political pressure to boost numbers joining the force.

Where thousands of officers are hired in such a short time scale, shortcuts are taken, core values may even be sacrificed in the name of expediency and inevitably mistakes are made allowing malign persons to slip through the process.

[4] https://www.defenseone.com/threats/2023/05/army-launches-recruiting-drive-cities-one-recruiter-lays-out-challenges/386435/

[5] https://www.abc.net.au/news/2023-05-17/police-recruitment-crisis-putting-community-at-risk/102304538

[6] https://www.nytimes.com/2022/11/13/opinion/us-police-military-extremism.html

[7] https://www.nytimes.com/2020/09/11/us/politics/veterans-trump-protests-militias.html

[8] https://apnews.com/article/us-military-racism-discrimination-4e840e0acc7ef07fd635a312d9375413

[9] https://www.express.co.uk/news/uk/1725327/met-police-Scotland-Yard-interviews-recruitment-latest-news-ont

Vetting is a time-consuming and largely manual process and resources are also constrained. A 2023 audit report on Security Vetting in the UK found that headcount was 23% behind what was required to meet vetting demand[10].

This is where automated, Straight Through Processing (STP) on background checks and security clearances can save significant time for recruiters, granting them more time for the necessary face-to-face engagement, thereby establishing a solid basis for hiring with confidence.

We are at the dawn of the Artificial Intelligence (AI) era and it will soon permeate all areas of modern life - including law enforcement and criminality. Security Vetting provides law enforcement agencies with an ideal opportunity to explore the value of AI, allowing the technology to contribute to completing rudimentary and repetitive tasks that impede the recruitment process.

This additional technological rigour also satisfies budgetary constraints by removing the need for additional headcount in processing applications while providing peace of mind to all stakeholders from a risk perspective.

[10] https://www.nao.org.uk/wp-content/uploads/2023/01/investigation-into-the-performance-of-uk-security-vetting.pdf - page 4 'Key Facts'

CLEARANCE BACKLOGS

Security clearance delays have almost been normalized as government institutions struggle with the challenge of leveraging technology to improve efficiency.

In Australia, the highly sensitive AUKUS nuclear submarine program being conducted in conjunction with the UK and US military is already swamped with a massive backlog of security clearances[11].

UK Security Vetting is currently implementing a delivery stabilization plan following what the National Audit Office labeled a significant deterioration in performance following the easing of COVID-19 restrictions.

One of the biggest challenges in processing security vetting is the time taken and the resulting backlogs caused by this time commitment.
In the UK:

Developed Vetting (DV) renewal processing averaged 255 days in 2022[12].

Nearly one-third of DV clearances in 2022-23 have taken more than 180 days to process, almost double UKSV's 95-day target, and backlogs exist.

(Supplied: Department of Defence)[11]

[11] https://www.abc.net.au/news/2023-03-31/defence-struggle-security-clearances-aukus-staff-rush/102167842

[12] https://www.nao.org.uk/wp-content/uploads/2023/01/investigation-into-the-performance-of-uk-security-vetting.pdf - page 8 'Key Findings'

AN AID TO DIVERSITY TARGETS

According to a March 2022 Ipsos poll, ethnic minorities are more likely to consider police officers (in the UK) racist compared to white people[13], while the same poll suggests women are less likely to think the police take violence against women and girls seriously in Britain compared to men. These views are not uncommon across different jurisdictions and are likely contributors to the lack of diversity within the police force and other such institutions.

In Australia, public sector unions have lamented the fact that applicants from overseas, or with family members overseas, have been excluded from graduate programs as they failed to get clearances from the Australian Government Security Vetting Agency[14].

Unfortunately, unconscious biases are factors in determining what a 'fit & proper' person might look like - even though the reality of real-time evidence might suggest shortlisted candidates who fit the right racial profile actually pose a greater threat to public safety. A layered, data-driven and thorough approach to 'whole person' applicant screening can contribute to a more equitable evaluation of candidates while also ensuring rogue applications are weeded out early.

While the emphasis on rigorous vetting may raise concerns about discrimination or bias, it is essential to recognise that a thorough vetting process can also be a tool for promoting diversity and inclusivity within security forces. By ensuring that the recruitment process is fair and free from bias, law enforcement and defense forces can attract a broader and more diverse pool of talent - hard data is key to diminishing such latent biases.

Diversity within the ranks brings a range of perspectives, experiences, and skills that can enhance the force's overall effectiveness. Moreover, it reflects the broader population that the security force serves, reinforcing the connection between these institutions and the civilian community.

[13] https://www.ipsos.com/sites/default/files/ct/news/documents/2022-05/uk-public-perceptions-of-local-policing-and-the-police-ipsos-april-2022.pdf

[14] https://www.abc.net.au/news/2023-02-10/dfat-accused-of-bungling-2023-graduate-program-recruitment/101954814

CONTRACTOR VETTING

The vetting process, of course, does not relate solely to employees and government bodies must be cognisant of existing relationships and potential threats when evaluating third-party contractors.

Contractors are embedded in many state law enforcement agencies due to deep sectoral knowledge but this ongoing reliance entails risk and also slows processing and decision-making. Most specialist contractors employ technical tools that can be considered complex. Therefore they are not necessarily accessible to frontline officers - in a world that relies on collaboration, software tools should be universally accessible (with appropriate access controls) and easy to navigate and use day-to-day for faster, accurate outcomes.

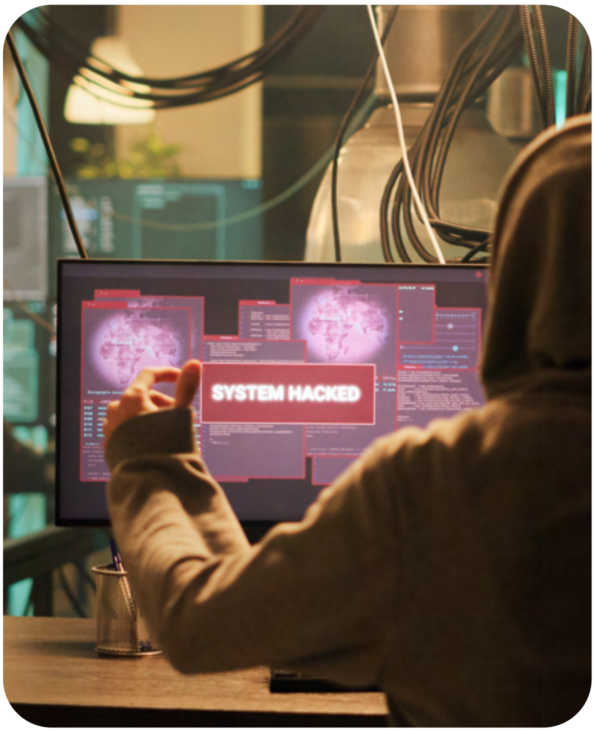
The threat to national security has shapeshifted in recent years with cybercrime, ransomware, denial of service and man-in-the-middle attacks now commonplace and new infiltration routes have emerged.

Foreign agents have widened the scope of their focus. As a consequence, the inter-dependencies and relationships between vendors must be known by procurement decision makers especially in a world where nefarious nation-state actors try to disrupt progress.

Earlier in 2023, Australian Security Intelligence Organisation secretary-general Mike Burgess spoke of the aggressive threat of espionage from multiple countries, focused not only on Australia's defence capabilities but on political and economic decision-making, academic research, critical infrastructure, innovation and personal information[15].

With such wide-ranging security threats, the need for vigilance and appropriate counter intelligence tools is intensifying.

This was again highlighted in May 2023, the Australian Federal Police were forced to defend how it manages conflicts of interests after it was discovered that a consulting firm it was investigating for criminal misuse of government information was also contracted as its internal auditor[16].



[15] https://www.asio.gov.au/director-generals-annual-threat-assessment-2023

[16] https://www.theguardian.com/business/2023/may/25/legal-constraints-hampering-australian-government-from-extracting-itself-from-pwc-contracts

PUBLIC PERCEPTION

Military servicemen and women are held in high regard by their compatriots. The virtues of honor, courage and self-sacrifice serve as beacons of inspiration to the civilian population.

This hard earned respect can be undermined however by extreme political affiliation, discriminatory behavior and deviation from ethical standards associated with defense forces which can create problems for line managers and the broader organization.

This is particularly evident when military and broader defense personnel air their personal views on social media accounts - either as themselves, as aliases or by endorsing the controversial views of third parties - their 'employer brand' is in the shop window, fuelling suspicion and undermining public confidence in the institutions they represent. Even the merest hint of intolerance or discriminatory behavior can have a negative impact on perception - without adequate technology and modern-day codes of conduct, handling this from a human resource perspective is an administrative impossibility.

FOSTERING PUBLIC TRUST

Public trust is an essential component of successful defense forces and national security agencies as well as local and federal police forces. Citizens must have confidence that the individuals tasked with their protection are both competent and trustworthy. Rigorous real-time vetting solutions not only ensure the competence and trustworthiness of personnel but also serve as a symbol of transparency and accountability.

Positively influencing public trust should be pre-emptive. When security forces are perceived as being selective and thorough in their recruitment and screening processes, it enhances public trust. Conversely, any perception of lax vetting can erode trust and lead to skepticism about the effectiveness and integrity of the establishment.

In democratic societies, where civilian oversight of law enforcement and military is paramount, public trust becomes even more critical. It is essential that defense forces are seen as institutions that serve the interests of the people rather than as entities that may harbor unscrupulous individuals.

IT SYSTEMS NEED TO EVOLVE TO MEET NEW REQUIREMENTS

Artificial Intelligence (AI) advances are rapidly disrupting how the world at large operates. The pace of IT system delivery for public institutions can appear glacially slow in an era of unprecedented and rapid technological evolution. Requirements change and by the time bespoke systems are delivered and implemented, they are often already dated. In order to get ahead of the curve in this era of rapid change, law enforcement bodies - and public service bodies more generally - must lean into cutting edge commercial expertise. Custom-built systems are more suited to long-established, mature operational functions like communications and payroll.

According to the National Audit Office report cited earlier in this document, the IT systems UKSV uses to process cases is old and unstable, with regular outages that slow down and stop the clearance process for extended periods. The IT system in question supports traditional vetting practices as intended but could not pre-empt the technological evolution resulting in the massive and complex modern day digital footprint of individual people. Therefore such systems simply cannot match the capabilities of a secure, scalable system like Siren which aggregates data from multiple sources into an easy-to-navigate, advanced analytics UI.

UKSV also acknowledges it has a heavy reliance on IT contractors despite deciding to move to a largely in-house approach after the failure of the previous attempt to reform the IT system.

Similarly in Australia, the AUKUS nuclear submarine program has been plagued by clearance delays where a new IT system for vetting has been besieged by technical difficulties since its introduction in late 2022.

The sheer scope of large scale IT infrastructure projects adds a huge additional workload for government agencies - but IT is not the core focus of these agencies nor should it be - and the delivery of such projects inevitably runs the risk of delay because these government agencies must focus their resources on their core priorities. Leveraging secure, trusted, specialist commercial systems reduces risk, hastens delivery and allows government institutions to perform their work without undue delay.

As one insider on the AUKUS Program reported to ABC News in Australia:

“There are massive backlogs of clearances for people wanting to go into the nuclear-powered submarine project – Defence cannot manage IT issues."

MODERN TOOL SET FOR A MODERN CHALLENGE

Essentially public trust and core value alignment within security forces is reliant on a Polaroid image in the digital age - a fading, hazy snapshot of a person's character that is increasingly out-dated and tells nothing of the life lived after that still photograph was taken. Like the fading Polaroid, the trust in the output of this archaic process is withering slowly.

Paper-based and timestamped form-based vetting solutions fail to take into account how a person's character and circumstances evolve over time. Once honest, credible people may fall on hard times; spiral into debt and/or substance abuse; moonlight in risky environments; cohabit with known criminals or accomplices or may even be radicalized - for a myriad of reasons - and this poses a direct threat to their motivations and how they conduct themselves at work. In fact, student loan debt was specifically highlighted as a potential risk in a study by RAND Corporation, so from the outset, a graduate with an otherwise pristine record who may truly exemplify the ethical standards required may still be vulnerable to foreign interference.

For the security of employees as well as the protection of communities and law and order, deployed IT systems must bring efficiency and reliability, enabling vetting staff to clear backlogs and bottlenecks that hamper delivery and workplace satisfaction.

17 https://www.abc.net.au/news/2023-03-31/defence-struggle-security-clearances-aukus-staff-rush/102167842

18 https://www.rand.org/pubs/research_reports/RRA757-1.html

A GLOBAL PERSPECTIVE

Vetting challenges are a global phenomenon affecting agencies across many security agencies. Social media poses a particular challenge - unlikely people can become radicalized, biases can be exposed and sometimes views can be misinterpreted and taken out of context[19].

Government employees are not unaffected by these challenges and vigilance is required. This vigilance requires technological tools for a technological problem. The cases below from global media outlets are indicative of the breadth and scale of the challenge.

Earlier this year (2023), a 21-year-old Massachusetts (US) Air National Guardsman with Top Secret/ Sensitive Compartmented Information clearance was arrested accused of leaking highly classified military documents[20]. A cursory look at social media and other records later illustrated repeated unsuitable behaviors that were not identified by background checks.

The Australian army has recently had to investigate neo-Nazis in it's ranks[21]. Threats are varied, omni-present and recurring and not isolated to defense forces.

The instances of misconduct and breaches of ethics in security forces come with a hefty price tag with the city of Chicago, IL alone paying $197.7m to resolve lawsuits relating to 1,000 police officers in a three year period[22].

In Victoria, Australia, Police Chief Commissioner Shane Patton had to address a rise in the number of police officers facing disciplinary hearings for misconduct including releasing confidential police information and public order offenses[23].

In Western Australia, in 2019, a 28-year veteran of the police force was found guilty of 180 data breaches and pornography offenses over a 10-year period after it was discovered that he had used police force computers to access sensitive personal information of 90 partners identified on data apps and website[24].

In 2023 concerns about vetting persist in the UK despite a 2022 police watchdog review which found cases of criminal behavior and links to criminality within the police force routinely overlooked. Previously, in 2019 the watchdog had estimated that 35,000 people working in police forces had not been adequately vetted.

In another troubling example, a 20-year veteran of the police force - later an armed officer in the diplomatic protection command was convicted of 49 separate counts of sexual offenses during his time in the police.

In the US, active law enforcement personnel (representing four states - New Jersey, Pennsylvania, Texas and Virginia) have been arrested and charged in connection with the January 6th (2021) insurrection at the US Capitol in Washington D.C.

[19] https://abcnews.go.com/US/dangers-social-media-law-enforcement-center-stage-amid/story?id=64252037

[20] https://www.nbcnews.com/politics/national-security/us-officials-identify-leaked-classified-documents-suspect-21-year-old-rcna79577

[21] https://www.smh.com.au/national/soldiers-of-hate-army-investigates-neo-nazis-in-its-ranks-20230314-p5crvv.html

[22] https://news.wttw.com/2023/08/22/repeated-police-misconduct-116-officers-cost-chicago-taxpayers-913m-over-3-years-analysis

[23] https://www.theage.com.au/national/victoria/i-make-no-apologies-patton-warns-police-to-behave-as-misconduct-complaints-rise-20230302-p5cot7.html

[24] https://www.perthnow.com.au/news/crime/ex-cop-adrian-trevor-moore-jailed-for-vetting-women-on-police-computer-ng-b881092029z

RECOMMENDATIONS

The contemporary world is marked by an ever-evolving array of security threats, encompassing conventional warfare, cyberattacks, terrorism, sabotage and espionage across all facets of life. It falls on defence and law enforcement agencies to counter these threats. In the face of these challenges, specialist technology must play an integral part in how security forces safeguard national security interests and protect law and order.

National security and law enforcement today is a data problem. With trillions of digital data points beyond traditional data sources used in vetting, the need for cutting edge technology is undeniable. For some, this may begin with addressing the knowledge gap - a prevalent lack of awareness of the technology available to counter these persistent threats.

Giving defense force hiring managers the tools to cross reference proprietary data with over 2000+ different data sources - in real-time - is a game changer for reducing vetting processing times, minimizing the risk of misconduct or abuse of power and boosting public perception.

When it comes to security vetting for government institutions, digital data must be at the heart of the process. Here are recommended best practices to reduce uncertainty and increase alignment to core values within security forces:
Real-time background checks - With straight through processing capabilities, days of manual work can be reduced to minutes, giving hiring managers the tools to hire with confidence.
Layered security clearances - layered checks that reach beyond traditional vetting to identify and flag more tenuous risks that can otherwise go unnoticed

Institutional policies - Regular review of institutional code of conduct and re-swearing of oath of office to reflect contemporary needs in the digital age (e.g. consent to review and monitor social media history)
Education - It is often said that the role of law enforcement rarely matches the recruitment brochure. Setting realistic expectations of the challenges faced and the importance of adherence to codes of conduct and regular monitoring to eradicate insider threats can contribute to a more positive culture and a more favorable public perception of these roles.
Budget Alignment - Provide adequate resources to reduce risk in recruitment and to counter heavily resourced nation-state actors. More often than not, this does not require additional funding as software offsets the need for additional headcount and retrospective PR campaigns.

25 https://www.standard.co.uk/news/london/met-police-vetting-rogue-officers-mark-rowley-watchdog-wayne-couzens-sarah-everard-b1080353.html

26 https://www.theguardian.com/commentisfree/2023/jan/16/the-met-police-rapist-david-carrick-failed-yet-again

27 https://www.bbc.com/news/uk-49847206

CONCLUSION

The need for rigorous vetting solutions within the defense forces, national security and law enforcement & corrections is paramount for upholding integrity and ethics, fostering public trust, mitigating insider threats, and promoting diversity and inclusivity.

Such institutions must continuously adapt to evolving security challenges, and the foundation of their strength and resilience lies in the caliber of their personnel and the tools at their disposal. In the digital age, the primary tool-set of this workload is specialist software.

Introducing new technology heralds change which can be perceived as daunting and there can be a collective resistance to stepping into new territory but as John F. Kennedy once said; “There are costs and risks to a program of action, but they are far less than the long range risks and costs of comfortable inaction.” Realizing the value of technological change requires action - the time to act and embrace the available technology is now.

Artificial Intelligence (AI) is on the cusp of unprecedented growth and will have a revolutionary impact on how information is processed and consumed. Law enforcement agencies must embrace these advancements and integrate quantum computing capabilities into day-to-day operations. Otherwise they run the risk of languishing behind the increasing sophistication of criminal enterprises in operational terms.

By implementing consistent, AI driven, technologically enhanced, agnostic vetting processes, decision makers can ensure that those who serve are not only competent but also unwavering in their commitment to their communities and to the core values of the institution they represent. In an era of complex and multifaceted security threats, rigorous real-time vetting is not just a choice; it is an imperative for the preservation of a nation's security, public trust in institutions and the protection of law and order.

WEB

WWW.SIREN.IO

EMAIL

INFO@SIREN.IO