DOCUMENT WHITEPAPER
STATUS PUBLIC
PAGES ~50
DATE MAY 2026

The Digital Infrastructure of Collective Efficacy.

A research paper examining the operational isolation of frontline security workers, the welfare and public-safety consequences of that isolation, and the case for a worker-first, alert-first communication network as a layer of urban intelligence.

Executive Summary

The modern private security industry is defined by a structural paradox. It deploys hundreds of thousands of trained, licensed professionals into the physical world every day, yet leaves them operationally isolated from one another. In the United Kingdom alone, the Security Industry Authority maintains over 400,000 active licences for frontline operatives who protect public spaces, retail environments, transport infrastructure, and critical national assets. Globally, the private security workforce exceeds 21 million personnel, significantly outnumbering state police forces in almost every major economy. Despite their numbers, these operatives work in silos, separated by employer boundaries, incompatible radio frequencies, geographic fragmentation, and a fundamental absence of shared digital infrastructure.

This isolation is not merely an operational inconvenience. It is a public safety failure with measurable consequences. Research from the University of Portsmouth indicates that approximately 40% of UK security operatives exhibit symptoms consistent with Post-Traumatic Stress Disorder, driven in large part by the psychological burden of lone working without peer support. Subsequent industry survey evidence has corroborated these findings, with practitioners reporting elevated incidence of physical violence and verbal abuse within preceding twelve-month reference periods. These individuals are the first point of contact in a crisis, yet they have no mechanism to warn each other, coordinate a response, or simply confirm that someone nearby is aware of their situation.

OnSiren is designed to end this isolation. It is not a security company. It is not a response service. OnSiren is an alert-first digital infrastructure platform that connects frontline workers into a unified, real-time awareness network. By leveraging geo-fenced channels and severity-based alert propagation, OnSiren digitises what sociologists call "collective efficacy"—the shared willingness of a community to intervene for the common good.

Crucially, OnSiren is not an employer-commissioned tool. It is a worker-first community app. Security officers download it themselves, on their own phones, and join the network as individuals. Employers cannot block it, and they do not need to approve it. The app provides a 24/7 professional identity for security officers—complete with NATO phonetic callsigns, a tactical sonar interface showing nearby nodes, and a premium black-and-gold aesthetic that elevates the profession. Officers use it on shift, off shift, and while commuting. They are always part of the network. They are always Watchers.

This white paper examines the anthropological foundations of collective vigilance, the mental health crisis facing lone workers, and the failure of legacy communication systems. It analyses the competitive landscape—including Project Griffin, Zinc/CityINTEL, Shopwatch radio networks, and the ACT counter-terrorism framework—and demonstrates how OnSiren differs from all of them. It presents detailed use cases for stadiums, shopping malls, Business Improvement Districts, and the gig economy. It maps the regulatory landscape across the UK, Europe, the United States, and the Gulf, and provides a comprehensive UK launch plan identifying the 341 active BIDs, 43 territorial police forces, and specific organisations OnSiren must partner with. Finally, it presents a full investor mapping, SWOT analysis, and PESTEL framework to guide strategic decision-making.

1. The Anthropological and Sociological Foundations

1.1 The Evolution of Collective Vigilance

Human survival has always depended on shared awareness. The capacity to detect threats and communicate them to others is not a modern invention; it is a fundamental evolutionary adaptation that predates language itself. The "Social Brain Hypothesis," proposed by anthropologist Robin Dunbar in 1998, argues that the human brain evolved its exceptional size primarily to manage complex social relationships and cooperative defence strategies. The central advantage of living in large social groups, Dunbar argued, was defence against predation. Communication and collective action were the mechanisms through which this advantage was realised.

This phenomenon of "collective vigilance" is observed across virtually all social species. In animal groups, individuals can reduce their personal state of hyper-vigilance when they are part of a larger collective, because they trust that others are also watching. The neuroendocrine stress response associated with isolation—elevated cortisol, sustained fight-or-flight activation—is measurably reduced when an individual perceives itself as part of a vigilant group. The biological imperative is clear: shared awareness reduces individual cognitive load and improves survival outcomes for the collective.

In human societies, this instinct was formalised into structures of collective security from the earliest settlements. The tribal watchfire—a communal flame maintained through the night—served as both a deterrent and a signal system. The medieval English system of the "Hue and Cry," codified in the Statute of Winchester (1285), legally obligated bystanders to raise an alarm and assist in apprehending criminals. In colonial Boston (1636), the first formal night watch was established, comprising community members who volunteered or were assigned to patrol the streets. The town crier served as the information broadcast system for entire communities—a single voice that could reach every ear within range.

Each of these systems shared a common architecture: immediate, peer-to-peer communication of threat information within a defined geographic area. They were, in essence, human sensor networks.

1.2 The Erosion of Natural Vigilance

In modern urban environments, this natural collective vigilance has been systematically eroded. The privatisation of public space, the professionalisation of security, and the fragmentation of communities have created artificial boundaries between the people who are physically present in the same location. Jane Jacobs, in her seminal 1961 work *The Death and Life of Great American Cities*, described the concept of "eyes on the street"—the natural surveillance that occurs when a neighbourhood is designed to encourage human presence and observation. Jacobs argued that safety emerges not from police patrols or surveillance cameras, but from the organic presence of attentive people who feel ownership over their shared space.

The modern security industry has inadvertently destroyed this organic vigilance by replacing it with isolated, employer-bounded silos. A security officer employed by G4S has no mechanism to warn a security officer employed by Securitas, even if they are standing fifty metres apart on the same high street. They are forced back into a state of isolated hyper-vigilance, bearing the cognitive load of threat detection entirely alone. The evolutionary advantage of collective awareness has been negated by organisational structure.

1.3 Digitising Collective Efficacy

In 1997, sociologists Robert Sampson, Stephen Raudenbush, and Felton Earls published a landmark study in the journal *Science* that introduced the concept of "collective efficacy." They defined this as "social cohesion among neighbors combined with their willingness to intervene on behalf of the common good." Their multilevel study of 343 neighbourhood clusters in Chicago—encompassing approximately 8,000 people each—demonstrated that neighbourhoods with high collective efficacy experienced up to 40% lower rates of violent crime, regardless of their socioeconomic composition.

The finding was profound: it was not wealth, policing levels, or physical infrastructure that determined safety. It was the shared perception among residents that their neighbours would act if something went wrong. A subsequent study by the National Institute of Justice in Miami-Dade County confirmed that residents with high perceptions of collective efficacy saw themselves as "protectors of their community," and that this shared cohesion directly reduced the fear of crime.

Albert Bandura's earlier work on self-efficacy (1982) provided the theoretical foundation: "Perceived collective efficacy will influence what people choose to do as a group, how much effort they put into it, and their staying power when group efforts fail to produce results." The critical insight is that collective efficacy is not static. It is a perception that can be built, reinforced, or destroyed by experience. A single successful collective intervention—a single moment where the network works—can dramatically shift perceptions upward.

OnSiren is the digital infrastructure of collective efficacy. It removes the friction of intervention. By providing a low-barrier mechanism to share information instantly with verified peers in a specific geographic radius, OnSiren enables a fragmented workforce to act as a cohesive community. It takes the innate human drive to warn others—the evolutionary imperative that kept our ancestors alive around the watchfire—and provides it with a frictionless digital conduit.

---

2. The Mental Health Crisis in Private Security

2.1 The Invisible Problem: Trauma and Isolation

The operational isolation of security personnel has severe psychological consequences that remain largely invisible to the public, to policymakers, and even to the industry itself. The private security workforce experiences levels of violence and trauma comparable to—and in some cases exceeding—

those of state police officers, yet without any of the institutional welfare support structures that police forces provide.

A comprehensive study by the University of Portsmouth, published as *Violence and the Mental Health of Security Operatives in the UK* (Talas, Button, Doyle, and Das, 2021, in *Policing and Society*), examined the experiences of 754 security operatives and revealed alarming statistics:

METRIC	FINDING
Physical assault in preceding 12 months	40% of respondents
Verbal abuse experienced monthly	Over 60% of respondents
Symptoms consistent with PTSD	Almost 40% of respondents
Monthly assaults (retail security specifically)	20% of retail security workers

These findings have been broadly corroborated by independent industry surveys conducted across comparable practitioner samples, which consistently identify the night-time economy, large events, and retail security as the sectors with the highest reported incidence of violence and abuse against operatives.

The researchers described this as "the invisible problem"—security workers' experiences are rarely captured in national crime statistics, their injuries are underreported, and their psychological distress goes largely unacknowledged. Unlike police officers, who have access to occupational health services, counselling, and peer support programmes funded by their force, private security operatives typically have no access to equivalent support. They process their trauma alone.

2.2 Persistent Traumatic Stress

Recent academic work has begun to reframe the psychological impact on frontline workers. Cogan (2026), writing in *Healthcare*, proposed the concept of "persistent traumatic stress" as distinct from the single-event model of PTSD. For security operatives, psychological distress is not caused by a single traumatic incident but by sustained, cumulative occupational exposure to hostility, violence, and threat. The lone working condition amplifies this: without peers to debrief with, without anyone to confirm that their experience was real and their response was appropriate, operatives internalise the stress without resolution.

The Health and Safety Executive defines lone workers as "those who work by themselves without close or direct supervision," and explicitly lists security officers as a high-risk category. The Canadian Centre for Occupational Health and Safety notes that isolated workers are at "greater risk for mental health concerns and loneliness" due to "limited contact with colleagues and separation from support networks."

2.3 The Evidence for Peer Support

Clinical research demonstrates that peer support is one of the most effective interventions for occupational trauma. A major systematic review by Shalaby and Agyapong (2020), published in *JMIR Mental Health* and cited 696 times, found that peer support—defined as "understanding another's situation empathically through the shared experience"—produces measurable positive effects on hope, recovery, and empowerment. It lowers the overall cost of mental health services and reduces re-hospitalisation rates.

The key principles of effective peer support are respect, shared responsibility, and mutuality. These are precisely the principles embedded in OnSiren's architecture. The app does not require officers to "open up" or engage in formal therapy. It simply connects them to others who share their experience. The knowledge that an alert will instantly reach nearby peers—that someone knows where you are and what you are facing—transforms the operative's experience from one of isolation to one of supported vigilance.

The app's sonar interface—a visual pulse that continuously scans the network and displays nearby active nodes as glowing yellow dots on a dark map—provides immediate, visceral confirmation that the operative is not alone. This is not a feature. It is a psychological intervention delivered through design.

2.4 The Role of Charities and the Current Gap

Charities such as Security Minds Matter (winner of Security Campaign of the Year 2023) are pioneering efforts to address the mental health crisis in the industry. However, their work is necessarily limited to awareness campaigns and signposting. They cannot solve the structural problem of isolation. The Suzy Lamplugh Trust, which pioneered lone worker safety advocacy in the UK, has long argued for better communication systems for isolated workers. Mind (the mental health charity) provides workplace programmes but has limited reach into the fragmented private security sector.

OnSiren does not replace these organisations. It provides the connective tissue that makes their work more effective. By reducing isolation at scale, OnSiren addresses the root cause of much of the psychological distress that these charities are trying to treat after the fact.

---

3. The Failure of Legacy Infrastructure

3.1 The Reporting Gap: ACT, CST, and See It Say It

Current counter-terrorism and community safety frameworks in the United Kingdom rely almost entirely on delayed, one-way reporting mechanisms that fail to provide real-time awareness to the people who need it most.

The UK government's Action Counters Terrorism (ACT) campaign instructs the public and professionals to report suspicious activity via a phone line (0800 789 321) or an online web form. The campaign's messaging—"Report it. Your call will not be recorded. You do not have to give your name"—is designed

to encourage reporting to authorities. But it provides no mechanism for alerting anyone nearby. A security officer who spots hostile reconnaissance outside a venue and calls the ACT hotline has done their civic duty. But the officer standing at the venue next door remains entirely unaware of the threat.

The Community Security Trust (CST), which protects the Jewish community, operates a similar model. Incidents are reported via phone (0800 032 3263), email (incidents@cst.org.uk), or web form. The CST recorded 3,700 antisemitic incidents in 2025. Their reporting system feeds into intelligence databases and maintains a Third Party Reporting status with the National Police Chiefs' Council. But it does not provide real-time alerting to nearby CST volunteers or community members.

The British Transport Police's "See It. Say It. Sorted." campaign relies on SMS texts to 61016. Again: one-way reporting to a central authority, with no feedback loop to the reporter and no alerting of nearby people.

The architecture of all these systems is identical:

STEP	CURRENT MODEL	ONSIREN MODEL
1	Person observes threat	Person observes threat
2	Person calls/texts/emails authority	Person triggers alert on OnSiren
3	Authority reviews report	Alert propagates to all nearby nodes instantly
4	No feedback to reporter	Reporter sees acknowledgments from network
5	No alerting of nearby people	Everyone in geo-fence is now aware
6	No collective response possible	Coordinated collective response enabled
7	Data sits in authority database	Data flows to police interface AND remains with network

The gap is fundamental. These systems were designed for intelligence gathering by the state. They were not designed for situational awareness on the frontline. OnSiren bridges this gap by ensuring that information flows laterally to peers first, while simultaneously creating the structured data record that can flow upward to central authorities.

3.2 The Limitations of Radio Networks (Shopwatch)

Business Improvement Districts and retail centres across the UK rely heavily on legacy two-way radio schemes, commonly known as Shopwatch. Research indicates that 83% of London BIDs use radio systems for their security communication. While these provide localised voice communication, they suffer from severe structural limitations.

The cost barrier is significant. Procuring handsets, maintaining repeaters, and paying Ofcom licensing fees makes these systems prohibitively expensive for many small businesses. Only individuals physically holding a radio handset are part of the network—a shopkeeper without a radio is entirely excluded from the intelligence loop, regardless of what they may observe. Communication is restricted

by the physical range of the hardware, and different retail centres or adjacent BIDs often operate on incompatible frequencies, preventing cross-district communication during a moving incident.

The result is a patchwork of disconnected islands. A shoplifter fleeing from one BID area into an adjacent one effectively disappears from the network. An active threat moving along a high street passes through multiple radio zones without any single network tracking its progress.

3.3 Top-Down Enterprise Platforms: Zinc and CityINTEL

Zinc Systems represents the enterprise approach to security communication. Its CityINTEL deployment —a branded version operated jointly by the City Security Council and the City of London Police— provides two-way information sharing between the Joint Command and Control Room (JCCR) and CSC member organisations. The platform is cloud-based, managed by police controllers, and capable of geofenced targeting of messages to specific buildings.

CityINTEL was launched in 2022 by Commissioner Angela McLaren and is powered by Zinc's Synapse platform. Its client base includes Allied Universal, ISS, Amazon Studios, Virgin Money, 22 Bishopsgate, and Graff Diamonds. It is a sophisticated tool for corporate security teams managing large sites.

However, CityINTEL and Zinc share a fundamental architectural limitation: they are top-down, employer-purchased, enterprise SaaS platforms. They require organisational procurement, lengthy sales cycles, and formal deployment. They connect corporate security teams to police, but they do not connect individual workers across different employers organically. A lone security officer working for a small contractor on a side street adjacent to 22 Bishopsgate has no access to CityINTEL unless their employer has purchased a licence.

The differentiation is structural:

DIMENSION	ONSIREN	ZINC/CITYINTEL
Adoption model	Worker downloads free app	Employer purchases enterprise licence
Network scope	All workers in a geographic area	Only workers whose employer has purchased
Cross-employer connection	Yes, by design	No, limited to contracted organisations
Cost to individual	Free	N/A (employer pays)
Speed to deploy	Instant (app download)	Weeks/months (procurement cycle)
Data generation	Bottom-up (from the street)	Top-down (from control room)

3.4 Project Griffin: The Concept Without the Infrastructure

Project Griffin, launched in April 2004 by the City of London Police and the Metropolitan Police, was a national counter-terrorism awareness initiative for the private security sector. It comprised three components: Awareness Days (training events), Bridge Calls (weekly intelligence conference calls), and Response (deployment protocols during emergencies).

The concept was validated dramatically during the 7 July 2005 London bombings, when Griffin-trained security personnel provided crucial support to overwhelmed emergency services—managing cordons, directing the public, and assisting casualties. The initiative spread internationally: Australia adopted it, Canada adopted it, Singapore created "Project Guardian," and the NYPD created "NYPD Shield."

However, Project Griffin's fundamental limitation was that it was training-only. It provided no persistent digital infrastructure to connect those trained officers after the training day ended. The Bridge Call was a weekly conference call—not real-time alerting. Between training events and weekly calls, Griffin-trained officers had no mechanism to communicate with each other. The network existed in theory but had no digital substrate.

Project Griffin was rebranded as ACT Awareness in 2018, following the recognition after the 2017 Manchester Arena and London Bridge attacks that awareness training alone was insufficient. OnSiren is the digital infrastructure that Project Griffin always needed—a way to keep the network alive, communicating, and generating intelligence continuously, long after the training day ends.

---

4. Learning from Precedents: Positive Case Studies

4.1 Citizen App: Proving Demand for Real-Time Awareness

The US-based Citizen App (formerly Vigilante, founded 2015) proved the massive, latent demand for real-time, localised safety information. Despite facing legitimate criticism for its early branding and the risks of unverified crowdsourced reporting, Citizen demonstrated several critical market truths.

During the George Floyd protests in June 2020, Citizen gained 600,000 new users in a single week, becoming the 7th most downloaded app in the United States. At its peak, the app served over 5 million active users across 60+ US cities. Firefighters and emergency medical personnel were documented using the app to navigate around active incidents because it provided faster situational awareness than their own dispatch systems.

The positive impact was measurable: during crises, people with access to real-time localised information made safer decisions. They avoided dangerous areas, they prepared for incoming threats, and they coordinated with neighbours. The app's investors—Sequoia Capital, Founders Fund, 8VC, Greycroft, and Lux Capital—collectively validated the thesis that real-time safety information is a venture-scale opportunity.

Citizen's failures, however, are equally instructive for OnSiren. The app relied on unvetted police scanner traffic and unverified user reports, which led to racial profiling, false accusations, and panic. In one notorious incident, Citizen offered a $30,000 reward for information on an innocent unhoused man mistakenly identified as an arsonist. The Electronic Frontier Foundation described the app as "crowd-sourced suspicion" that was "out of control."

OnSiren avoids these pitfalls entirely through its architectural choices. It uses trained, licensed professionals rather than the general public—eliminating the racial profiling risk. It is alert-first with

structured data (type, location, severity) rather than unverified commentary. It operates through geo-fenced channels with verified membership rather than open city-wide feeds. It connects to police through structured data interfaces rather than raw 911 monitoring.

4.2 Zello: Ad-Hoc Infrastructure in Crisis

Zello, the Austin-based push-to-talk smartphone app founded in 2011, demonstrated the power of digital radio networks to replace traditional hardware. With over 100 million registered users and $23.5 million in annual recurring revenue achieved with a staff of approximately 20 people, Zello proved that smartphone-based voice networks can achieve massive scale.

The defining moment came during Hurricane Harvey in 2017, when the "Cajun Navy"—a volunteer rescue group—used Zello as their primary coordination tool for civilian rescue operations. At the peak of the crisis, Zello was adding 7,000 new users per minute. The app topped app store charts and demonstrated that in moments of genuine emergency, people will adopt whatever tool provides immediate peer-to-peer communication.

Zello's growth model, analysed by Reforge, revealed several principles directly applicable to OnSiren. Its group/channel orientation (rather than one-to-one messaging) led to faster viral spread with a higher branching factor. Its targeting of underserved markets—people who cannot sit at keyboards (drivers, construction workers, security personnel)—tapped into massive unmet demand. Its bottoms-up adoption model meant that free users became mini-sales representatives for enterprise deals, as they introduced the tool into their workplaces organically.

The key lesson: Zello proved that PTT on smartphones works at scale. But Zello's limitation is that push-to-talk is all it does. It has no alert layer, no severity propagation, no geo-fencing, and no structured data generation. OnSiren adds the intelligence layer that Zello lacks—the alert that travels faster than voice, reaches further than a single channel, and generates data that can be analysed and shared.

4.3 Rave Mobile Safety: Institutional Scale

Rave Mobile Safety (founded 2004, acquired by Motorola Solutions in 2022) demonstrated that safety communication platforms can achieve institutional scale. Before its acquisition, Rave served 8,000 contracted clients, 1,800 higher education institutions, 10,000 K-12 schools, and 3,000 public safety agencies, covering over 50 million individuals across all 50 US states. It achieved 11 consecutive years of double-digit revenue growth and earned FedRAMP authorisation (the US government's highest security certification for cloud services).

Rave's architecture was top-down: institutions send mass notifications to individuals via text, email, voice, and desktop alerts. Its Panic Button product enabled one-touch alerting in schools. Its Smart911 product allowed citizens to create safety profiles visible to dispatchers during emergency calls.

The acquisition by Motorola Solutions—the world's largest provider of mission-critical communications—validated the entire category. It proved that safety communication infrastructure is worth billions and that incumbents will pay premium prices to acquire it.

OnSiren's advantage over Rave is architectural: Rave is top-down (institution broadcasts to people). OnSiren is bottom-up (people on the ground generate intelligence upward). Rave requires institutional procurement. OnSiren requires only an individual downloading an app. Rave covers people passively (they receive alerts). OnSiren activates people as nodes (they generate alerts). This bottom-up model creates a data asset that top-down systems cannot replicate.

---

5. The OnSiren Architecture: How It Works

5.1 Alert-First, Talk-Second

OnSiren is not a walkie-talkie. It is not a messaging app. It is an alert network with voice capability. This distinction is fundamental to understanding its architecture and its differentiation from every competitor in the market.

The atomic unit of value in OnSiren is the alert. An alert is a structured data object comprising type (shoplifting, assault, suspicious behaviour, active threat), location (precise GPS coordinates within a geo-fenced zone), severity (which determines propagation radius), and optional voice annotation. An alert can be triggered with a single tap. It requires no typing, no explanation, and no conversation. It simply broadcasts: something is happening, here, now.

Push-to-talk exists as a secondary capability for coordination after the initial alert. Once nearby officers are aware of the situation, they can use PTT to discuss response—"I can see him, he's heading toward the tube station," or "I'm coming to you, stay where you are." But the alert travels first, at the speed of a push notification, reaching every node in the geo-fence before any voice communication begins.

This architecture reflects the reality of crisis situations. In the first seconds of an incident, an officer does not have time for a conversation. They need to broadcast. The alert is that broadcast—immediate, structured, and impossible to miss.

5.2 Geo-Fenced Channels: Geography, Not Organisations

OnSiren's channels are defined by geography, not by employer. When a security officer opens the app, they are automatically placed in the channel corresponding to their physical location. Every other officer in that zone—regardless of which company employs them, which site they are assigned to, or which uniform they wear—is in the same channel.

This is the critical architectural decision that breaks the organisational silo. A G4S officer and a lone operator and a Mitie employee and an in-house retail security guard, all working within the same 500-metre radius, are all on the same channel. They can hear each other. They can warn each other. They can see each other on the sonar.

The geo-fence boundaries are configurable. A high street might be a single zone. A shopping mall might be its own zone. A stadium during an event creates a temporary zone that encompasses the venue and

its surrounding approach routes. The system is dynamic—zones can be activated, expanded, or contracted based on events, time of day, or threat level.

5.3 Severity-Based Alert Propagation

The most innovative element of OnSiren's architecture is its severity-based propagation model. Not all alerts are equal, and not all alerts should travel the same distance.

A low-severity alert—"shoplifting suspect, male, blue jacket, heading east on Oxford Street"—propagates within the immediate geo-fence only. Officers in the adjacent zone may not need this information. It is localised, tactical, and time-sensitive.

A high-severity alert—"active threat, knife attack, Regent Street"—propagates outward to the entire city. Every officer in every zone within the metropolitan area receives it. The blast radius of information matches the blast radius of the threat.

This tiered propagation model mirrors how real emergencies work. Local incidents require local awareness. Major incidents require city-wide awareness. The system makes this determination based on the alert type selected by the triggering officer, with the potential for AI-assisted classification in future iterations.

5.4 The Sonar: Visual Proof of the Network

The OnSiren interface is built around a central visual metaphor: the sonar. On a dark map background, the user's position is marked by a central pulse—a red-orange dot with an expanding ring, like a radar sweep. Surrounding this central point, nearby active officers appear as glowing yellow dots, scattered across the map in real-time.

This is not merely a design choice. It is a psychological intervention. The sonar provides immediate, visceral proof that the officer is not alone. Before they send an alert, before they use PTT, before they do anything at all, they can see the network around them. The yellow dots are other professionals—trained, licensed, present, and connected. The isolation that defines the current experience of security work is replaced, at a glance, by visible community.

The aesthetic is deliberately tactical and premium. The colour palette—black background, yellow/gold for friendly nodes, red for threats—evokes both high-visibility safety equipment and military-grade command systems. NATO phonetic alphabet callsigns (ALPHA-9, BRAVO-47, CHARLIE-21) replace real names, providing both operational security and a sense of professional identity. The overall effect communicates: this is not a consumer app. This is professional infrastructure that happens to be beautiful.

5.5 Alpha One: AI Net Control

OnSiren's AI assistant, designated Alpha One, serves as an automated net controller. Alpha One briefs officers at the start of their shift with relevant intelligence from the preceding period—what happened in their zone, what alerts were raised, what patterns emerged. It monitors officer welfare through activity detection and can trigger welfare checks if an officer goes silent for an extended period. It provides

contextual information during incidents, drawing from the network's historical data to inform real-time decision-making.

Alpha One does not replace human judgment. It augments it. In a crisis, when cognitive load is at its highest, Alpha One handles the administrative burden—logging the alert, notifying the police interface, tracking the timeline—so that the officer can focus entirely on the situation in front of them.

5.6 OnSiren Mobile: The Roaming Sensor

OnSiren Mobile is a physical vehicle—equipped with LiDAR-type scanning technology—that travels through city streets collecting environmental and situational data. This data feeds directly into the network, enriching the intelligence available to officers in each zone.

The vehicle acts as a ground-truth verification layer. While human-generated alerts provide real-time incident data, OnSiren Mobile provides ambient environmental intelligence: crowd density, unusual patterns of movement, vehicle anomalies, and changes to the physical environment. This data keeps street-level networks cleaner and more accurate, reducing false positives and providing context for human-generated alerts.

---

6. The Worker-First Distribution Model

6.1 Why Not Start with Employers

The conventional approach to enterprise security software is to sell to the employer. Zinc does this. CityINTEL does this. Every legacy radio system does this. The employer purchases the system, deploys it to their staff, and controls the network.

OnSiren deliberately inverts this model. It goes directly to the individual security officer. The officer downloads the app themselves, on their own phone, and joins the network as an individual. This is not a tactical choice driven by sales efficiency. It is a strategic decision rooted in three fundamental insights.

First, employer procurement cycles are slow. A decision to adopt a new communication platform in a large security company involves procurement teams, IT security reviews, union consultations, and budget approvals. This process takes months or years. Going direct to the officer takes seconds.

Second, employer-controlled networks cannot be cross-employer by definition. If G4S deploys a communication tool to its staff, that tool connects G4S officers to other G4S officers. It does not connect them to Securitas officers, Mitie officers, or lone operators. The entire value proposition of OnSiren—breaking the organisational silo—is impossible within an employer-controlled architecture.

Third, employer-controlled networks create a dependency that undermines trust. If the employer can see everything an officer says and does on the platform, officers will self-censor. They will not report concerns about their own working conditions, they will not flag welfare issues, and they will not use the

platform as a genuine peer support network. Worker-first ownership creates the psychological safety necessary for authentic engagement.

6.2 Legal Positioning: Why Employers Cannot Block It

The legal framework in the United Kingdom strongly supports the right of workers to use personal safety tools on their own devices. Under Section 2 of the Health and Safety at Work etc. Act 1974, employers have a duty to ensure, so far as is reasonably practicable, the health, safety, and welfare of their employees. Under the same Act, employees have a corresponding duty to take reasonable care of their own health and safety.

An employer who attempted to prevent a security officer from using a personal safety app on their own phone would face significant legal exposure. The employment tribunal case *Alsnih v. Al Quds Al-Arabi Publishing & Advertising* established that employers cannot force employees to install work-related apps on personal phones, and by logical extension, they cannot prevent employees from installing personal safety apps on their own devices.

Furthermore, the Management of Health and Safety at Work Regulations 1999 require employers to conduct risk assessments for lone workers and implement "reasonably practicable" measures to mitigate identified risks. If a worker independently adopts a safety tool that demonstrably reduces their risk, and the employer actively prevents them from using it, the employer is arguably failing in their duty of care. Should that worker subsequently be harmed in a situation where the app could have provided warning or assistance, the employer's liability would be severe.

The Corporate Manslaughter and Corporate Homicide Act 2007 adds further weight. Penalties under this Act start at £300,000 with no maximum limit. Companies with turnover exceeding £50 million can face fines of up to £20 million. In 2017, a London local authority was fined £100,000 after a lone social worker was assaulted on a home visit. A utility company was fined £1.8 million after a lone worker fatality. The legal environment is clear: obstructing worker safety is not merely ethically indefensible—it is financially catastrophic.

6.3 The Terms: OnSiren and the Individual

The relationship between OnSiren and the security officer is direct, personal, and permanent. The officer's account belongs to them, not to their employer. Their callsign is theirs. Their network connections are theirs. If they change employers, their OnSiren identity persists. If they are between contracts, they remain part of the network.

This creates a professional identity layer that transcends employment. In an industry characterised by high turnover, zero-hours contracts, and frequent employer changes, OnSiren provides the one constant: a persistent professional community that recognises the officer's existence regardless of their current contract status.

6.4 Off-Duty Usage: The 24/7 Watcher

OnSiren is not an app that officers use only at work. It is a community app for security professionals that they carry with them at all times. An off-duty officer commuting home through a high street is still a

trained observer. They still notice things that untrained civilians miss. Their professional instinct does not switch off when their shift ends.

By enabling off-duty usage, OnSiren elevates the status of the security professional. They are not merely employees performing a function during contracted hours. They are members of a professional community with a permanent identity and a permanent role. The app's premium aesthetic—the tactical black-and-gold design, the NATO callsigns, the sonar interface—reinforces this elevated status. It communicates: you are a professional. You are part of something. You matter.

This off-duty engagement also generates invaluable data. Officers travelling through different zones provide ambient network density even outside their working hours. They extend the coverage of the network into times and places that would otherwise be dark. The network becomes truly persistent—not dependent on shift patterns or employer deployment schedules.

---

7. The Watchers: Expanding Beyond Security Officers

7.1 The Two Layers: Guards and Watchers

OnSiren's long-term vision extends far beyond licensed security officers. The network has two conceptual layers:

The Guards are licensed security professionals. They are trained to respond. They hold SIA licences. They are deployed to specific sites. They are the backbone of the network—the verified, trusted nodes that anchor the system's credibility.

The Watchers are the broader frontline workforce. Shopkeepers, Uber drivers, bus drivers, delivery riders, hotel receptionists, bar staff, taxi drivers, street cleaners. They are not trained to respond. They are not expected to intervene. But they observe. They notice. They can send an alert when they see something that concerns them. They extend the network's coverage into every street, every vehicle, every shop counter.

The Guards talk. The Watchers listen and alert. Both generate data. Together, they form a comprehensive human sensor network that covers every inhabited space in a city.

7.2 The Gig Economy: A Natural Fit

The gig economy workforce represents a massive, underserved market for peer safety networks. Uber drivers, Deliveroo riders, DoorDash couriers, and their equivalents globally operate in conditions strikingly similar to lone security workers: they work alone, they move through unfamiliar areas, they interact with strangers, and they face elevated risk of assault and robbery.

Current safety infrastructure for gig workers is reactive and individual. Uber's integration with RapidSOS allows a driver to swipe an emergency button that shares their location and vehicle details with 911 dispatchers. Deliveroo riders can flag safety concerns in-app. But none of these systems connect

workers to each other. A Deliveroo rider being followed through a dark street cannot alert other riders nearby. An Uber driver in a dangerous neighbourhood cannot see if other drivers are in the vicinity.

This is precisely the gap OnSiren fills. The peer safety layer that sits underneath all gig platforms. Riders and drivers do not need push-to-talk. They need to receive alerts ("robbery in progress, avoid Elm Street") and send alerts ("I'm being followed, junction of Park Road and High Street"). The geo-fenced channel model means they are simply added to the same zones as security officers. The network becomes denser, the data becomes richer, and the coverage becomes comprehensive.

7.3 Shopkeepers: The Fixed Nodes

Shopkeepers represent the ideal "fixed node" in the Watchers network. They are stationary, they have clear sightlines to the street, they observe patterns over time, and they are frequently the first victims of crime. A local shopkeeper who notices the same individual conducting hostile reconnaissance over several days has intelligence that no CCTV camera can provide—contextual, pattern-based human observation.

Currently, shopkeepers in BID areas may have access to a Shopwatch radio if their BID provides one. But the majority do not. They are excluded from the intelligence loop entirely. OnSiren includes them for free. A shopkeeper downloads the app, joins their zone, and immediately begins receiving alerts from nearby security officers. They can also generate alerts themselves—"shoplifter heading east, male, red hoodie"—that reach every officer and every other shopkeeper in the zone.

The question of whether Harrods can have it and a local corner shop can also have it is answered by the architecture itself: yes. Both are nodes in the same geo-fenced zone. Both receive the same alerts. Both can contribute intelligence. The network does not discriminate by the size of the business. It discriminates only by geography.

7.4 Transport Workers: The Mobile Nodes

Bus drivers, taxi drivers, and transport workers represent the mobile layer of the Watchers network. They move through multiple zones during a single shift, providing dynamic coverage and real-time intelligence about conditions across a wide area. A bus driver who observes a disturbance at a stop can alert security officers in that zone instantly—without stopping, without calling anyone, without filling in a form.

Transport for London alone employs thousands of bus drivers covering every major route in the capital. Black cab drivers number approximately 21,000 in London. Private hire drivers number over 90,000. Each one is a potential mobile node, moving through the city with trained observational awareness and a professional interest in the safety of their operating environment.

7.5 The Scale of the Opportunity

When the Guards and the Watchers are combined, the addressable network in the UK alone is substantial:

CATEGORY	ESTIMATED UK WORKFORCE
Licensed security officers	400,000+
Retail workers (customer-facing)	2,900,000
Hospitality workers	1,800,000
Gig economy drivers/riders	1,000,000+
Bus drivers	135,000
Taxi/private hire drivers	362,000
Street-facing public sector workers	500,000+
Total addressable network	**7,000,000+**

Globally, the numbers are transformative. The United States alone has 1.1 million private security guards, 1.4 million ride-share drivers, and millions of retail and hospitality workers. India has over 7 million private security personnel. The Gulf states are investing billions in smart city infrastructure that requires exactly this kind of human sensor network.

---

8. Detailed Use Cases

8.1 Wembley Stadium: 90,000 People, One Network

Wembley Stadium currently uses a MOTOTRBO digital radio system (Motorola Solutions) with 80 emergency stewards' phones linked via a dedicated fire alarm system. A stadium control room coordinates communications with steward supervisors via radio. During a major event, thousands of stewards, security officers, police officers, and venue staff must coordinate the safety of 90,000 attendees.

OnSiren's geo-fenced channel model is ideally suited to this environment. A temporary event zone is created encompassing the stadium and its approach routes. Every security officer, steward, and police officer with the app is automatically placed in this channel for the duration of the event. Alerts propagate instantly to all personnel—"crowd surge at Gate D," "medical emergency Section 114," "suspicious package North-West concourse."

The advantage over traditional radio is threefold. First, there is no hardware to distribute and collect. Officers arrive with their phones already connected. Second, the network is not limited to those issued radios—every officer with the app is included. Third, the data generated during the event (alert types, response times, incident locations) provides the venue with intelligence for future event planning that radio systems cannot capture.

8.2 Shopping Malls: Multi-Tenant Coordination

A large shopping mall such as Westfield Stratford City contains hundreds of individual retail units, each with their own staff, plus a central mall security team, plus external security contractors, plus police officers on patrol. These groups currently operate in complete isolation from each other. The mall security team has radios. Individual retailers may have their own internal communication. Police have Airwave. None of these systems interoperate.

OnSiren creates a single geo-fenced zone for the mall. Every security officer (regardless of employer), every shop manager who downloads the app, and every police officer who opts in is on the same channel. A shoplifting alert from one retailer instantly reaches the security team at every exit. A violent incident in one unit triggers awareness across the entire complex. The mall operates as a single coordinated entity rather than a collection of isolated businesses.

8.3 Business Improvement Districts: Replacing Radio with Network

The United Kingdom has approximately 341 active Business Improvement Districts, with over 70 in London alone. BIDs charge a levy on all business rate payers and provide services including security, cleaning, and marketing. Security is consistently ranked as a top priority by BID members, and the majority of BIDs invest in radio schemes (Shopwatch), CCTV, and intelligence-sharing platforms such as DISC.

OnSiren offers BIDs a transformative proposition: replace expensive radio hardware with a free app that connects not only the BID's contracted security team but every business in the district. The BID manager receives a command-and-control dashboard (paid tier) showing real-time network activity, alert history, and coverage maps. The police receive a structured data feed of verified alerts. Individual businesses receive alerts relevant to their zone without purchasing any hardware.

The cost saving alone is compelling. A typical Shopwatch radio scheme costs £15,000-£50,000 annually in hardware, maintenance, and licensing. OnSiren replaces this with a free app for individual users and a modest SaaS fee for the BID's management dashboard. The coverage is superior (every smartphone is a node, not just those with radios), the data is richer (structured alerts with metadata vs. ephemeral voice), and the network is larger (every willing participant, not just those issued hardware).

8.4 Football Matches: Dynamic Event Security

Football matches present a unique security challenge: large crowds, rival factions, alcohol, and predictable flashpoints (arrival, half-time, departure). Currently, match-day security relies on stewards with radios, police with Airwave, and CCTV operators in a control room. These systems do not connect to each other seamlessly, and they certainly do not connect to the broader community of security professionals, transport workers, and retailers in the surrounding area.

OnSiren enables a dynamic event zone that activates on match day and encompasses the stadium, surrounding pubs, transport hubs, and approach routes. Security officers at the venue, police on patrol, transport staff at nearby stations, and pub door supervisors are all on the same channel. An alert about a group of aggressive fans leaving a pub reaches the stadium security team before the group arrives. An incident inside the ground reaches transport staff who can prepare for disrupted crowd flows.

8.5 Critical National Infrastructure

Hospitals, power stations, water treatment facilities, government buildings, and transport hubs all require security that coordinates with police and emergency services. The Terrorism (Protection of Premises) Act 2025 (Martyn's Law) specifically identifies these as Enhanced Tier premises requiring formal public protection procedures.

OnSiren's police interface capability—structured data flowing from the network to law enforcement systems—positions it as a compliance tool for Enhanced Tier venues. The Act requires these premises to have procedures for "monitoring of the premises and its immediate vicinity" and "communication and coordination with relevant authorities." OnSiren provides both: the monitoring is performed by the human network, and the communication flows through the structured data interface.

---

9. Impact and Urban Intelligence

9.1 The Three Effects of Connection

If the architecture proposed in this paper achieves meaningful penetration, three distinct categories of effect should be expected. They are presented here as falsifiable hypotheses rather than asserted outcomes; each is accompanied by an indication of how it would be evaluated.

The first is a *welfare effect*. The literature on social isolation and occupational mental health is extensive and broadly consistent: workers who lack reliable peer contact during their working hours report elevated rates of stress, anxiety, and burnout, and are more likely to leave the profession. Large meta-analyses, including Holt-Lunstad and colleagues' 2023 review of workplace interventions, report that interventions which raise perceived social support produce small but consistent improvements in self-reported wellbeing and work ability. The hypothesis is that a persistent, low-friction peer-awareness layer between operatives, sustained across shifts and across employers, should raise self-reported sense of belonging and reduce the felt isolation of lone working. The appropriate evaluation is a pre-registered, multi-site comparison of operators with and without active network coverage over at least six months, with self-report instruments and routinely collected operational data as outcomes.

The second is a *district-level efficacy effect*. The Sampson, Raudenbush and Earls (1997) framework predicts that an environment in which informal observers can act on the common good will display measurably lower rates of violence and disorder than one in which they cannot. The Chicago Project on Human Development found a roughly 40 per cent reduction in interpersonal violence associated with high collective efficacy after controlling for socio-economic status. Whether a digitally mediated peer-awareness layer can produce comparable effects in a contemporary urban setting is, on the evidence, unsettled. The expected magnitude is smaller than the Sampson estimates and likely uneven across contexts, but the directional prediction is the same: in districts with sustained network density, indicators of disorder, fear of crime, and reactive policing demand should decline relative to matched comparison districts.

The third is a *crisis-mobilisation effect*. There is now a small but suggestive evidence base on what happens when a smartphone-mediated peer network is overlaid on an existing trained workforce in moments of crisis. During Hurricane Harvey in 2017, the Cajun Navy used Zello as a coordination layer for civilian rescues, with peak channel concurrency well above sustained levels and rescue volumes that the literature credits in part to the network. During the 2020 protests in major US cities, the Citizen application reported a near-fivefold increase in active users in a single week. Waze for Cities, originally a navigation product, became infrastructure for hundreds of municipal authorities once they recognised the operational value of crowd-sourced reporting. The common feature is not the technology, but the principle: a pre-existing trained group plus a low-friction reporting layer compounds capacity faster than either component alone.

9.2 The Police Interface

The argument for a structured interface to police is principally that the network would otherwise generate evidence of risk that fails to reach the institutions best placed to act on it. If officers across multiple employers are issuing aligned alerts about a single individual or vehicle in a defined geographic area, that pattern is informative whether or not any individual alert meets the threshold for a 999 call. A police-facing read-only feed, governed by appropriate data-sharing agreements and aligned to the National Business Crime Centre data-sharing framework, is the obvious mechanism. The careful design choice is to make the interface read-only and partner-controlled rather than enforcement-led: the platform is not an instrument of state surveillance, but an information layer whose users include law enforcement.

9.3 Adjacent Workforces

The analysis presented in earlier sections has focused on licensed security operatives. The concept of a peer-awareness layer is, however, plausibly extensible to a broader population of frontline workers whose conditions of work share two characteristics: physical presence in public space and exposure to elevated occupational risk. The principal candidate populations in the United Kingdom are taxi and private-hire vehicle drivers (estimated at over 350,000 licensees), large-fleet delivery riders associated with platforms such as Deliveroo, Just Eat and Uber Eats (estimated at over 120,000 active riders), public-service bus drivers (approximately 130,000), Royal Mail postal staff (approximately 130,000), and a long tail of retail, hospitality and transport workers whose roles place them in direct public contact. The aggregate population is in the order of two million in the United Kingdom alone. Comparable populations exist in every major economy.

We are explicit that extension to these populations carries design and governance implications that the security-only deployment does not. The verification model differs (employer attestation rather than SIA licence), the trust architecture must be more conservative (with stronger anti-vigilantism protections), and the alert-propagation logic requires recalibration for non-trained nodes. None of these challenges is fatal, but each requires careful product work before extension is responsible.

9.4 Urban Intelligence as a New Layer

If the architecture proposed in this paper achieves the network density we have described, what emerges is, in our view, a new operational layer of urban intelligence. The closest analogue is the role

that real-time traffic data has come to play in city operations over the past two decades. Before Waze, INRIX, and TomTom, congestion was understood through retrospective sensor data and modelled estimates; the lived experience of drivers was invisible to planners. The introduction of crowd-sourced, real-time data did not replace existing instruments, but added a complementary layer that has progressively reshaped routing, signal management, incident response, and infrastructure investment. The proposition advanced here is that frontline-worker observation could play an analogous role for the live state of public-space safety. We are explicit that this is a directional claim rather than a confident prediction; the technology is at an earlier stage than the traffic analogue, and substantial empirical work would be required to substantiate it.

---

10. Regulatory Alignment: Martyn's Law and Beyond

9.1 The Terrorism (Protection of Premises) Act 2025

The Terrorism (Protection of Premises) Act 2025—commonly known as Martyn's Law, named after Martyn Hett, one of the 22 people killed in the Manchester Arena bombing of 2017—received Royal Assent on 3 April 2025 and will come into force within 24 months (by April 2027). It represents the most significant piece of protective security legislation in the UK in decades.

The Act creates two tiers of obligation:

Standard Tier applies to premises and events with a capacity of 200 or more people. Responsible persons must implement "public protection procedures" that are "reasonably practicable." These procedures must include measures to reduce vulnerability to terrorist attacks and reduce harm in the event of an attack. The Act does not prescribe specific technologies but requires that procedures be documented, communicated to relevant staff, and reviewed regularly.

Enhanced Tier applies to premises and events with a capacity of 800 or more people. In addition to Standard Tier requirements, responsible persons must implement "public protection measures" including monitoring of the premises and its immediate vicinity, physical measures to reduce vulnerability, and communication and coordination arrangements with relevant authorities.

The Security Industry Authority (SIA) has been designated as the regulator for Martyn's Law compliance, with powers to inspect, enforce, and penalise non-compliance.

9.2 OnSiren's Compliance Positioning

OnSiren should position itself using the exact language of the legislation. The following terminology should be embedded in all product documentation, marketing materials, and sales conversations:

LEGISLATIVE TERM	ONSIREN EQUIVALENT
Public protection procedures	OnSiren's alert and communication protocols

LEGISLATIVE TERM	ONSIREN EQUIVALENT
Public protection measures	The geo-fenced network as a monitoring measure
Reasonably practicable	Free app requiring no hardware investment
Monitoring of premises and vicinity	Real-time human sensor network
Communication and coordination with authorities	Police data interface
Duty holder	The responsible person at each qualifying premises

The "reasonably practicable" standard is particularly important. Under UK health and safety law, a measure is reasonably practicable if the cost of implementing it is not grossly disproportionate to the risk it mitigates. OnSiren is free for individual users and low-cost for organisations. It is difficult to argue that adopting a free safety tool is not "reasonably practicable."

9.3 The April 2027 Deadline: A Regulatory Catalyst

The 24-month implementation period creates a hard deadline by which every qualifying premises in the UK must have documented public protection procedures in place. This affects an estimated 155,000 premises across the country. Each of these venues will be actively seeking solutions that demonstrate compliance.

OnSiren's timing is optimal. Launching now—12 months before the compliance deadline—provides sufficient time to build network density and establish credibility before the regulatory pressure peaks. By April 2027, OnSiren should be positioned as the default tool that venues can point to as evidence of their "reasonably practicable" communication and coordination measures.

9.4 International Regulatory Equivalents

The UK is not alone in strengthening protective security legislation. Several international markets have equivalent or emerging frameworks:

France implemented the Vigipirate plan following the 2015 Paris attacks, requiring businesses in crowded places to implement security measures. The 2017 SILT law (Strengthening Internal Security and the Fight Against Terrorism) made permanent many emergency powers and imposed security obligations on event organisers.

Australia developed the "Australia's Strategy for Protecting Crowded Places from Terrorism" (2017, updated 2024), which provides a framework for owners and operators of crowded places to understand and mitigate the threat of terrorism. While not yet legislated as mandatory (unlike Martyn's Law), it creates strong expectations.

Singapore created Project Guardian (adapted from Project Griffin) and maintains the Infrastructure Protection Act, which imposes security obligations on designated critical infrastructure.

United States operates under the Department of Homeland Security's "Soft Targets and Crowded Places" framework and CISA's infrastructure protection guidelines. While there is no single federal equivalent to Martyn's Law, individual states and cities impose security requirements on venues, and the legal liability environment (civil lawsuits) creates strong incentives for proactive security measures.

European Union is developing the EU Protective Security Framework, which may harmonise requirements across member states. The EU Counter-Terrorism Agenda (2020) specifically calls for better protection of public spaces and improved information sharing between private security and law enforcement.

Each of these markets represents an opportunity for OnSiren to position itself as a compliance tool that helps venues and organisations meet their protective security obligations.

---

11. The International Growth Playbook

10.1 Market Prioritisation Framework

OnSiren's international expansion should be guided by three criteria: the size of the private security workforce, the strength of duty-of-care legislation, and the presence of a regulatory catalyst equivalent to Martyn's Law. Markets that score highly on all three criteria should be prioritised.

MARKET	WORKFORCE SIZE	DUTY OF CARE STRENGTH	REGULATORY CATALYST	PRIORITY
United Kingdom	400,000+	Very Strong (HASAWA)	Martyn's Law 2027	**Launch market**
United States	1,100,000+	Strong (OSHA)	Civil liability culture	**Year 2**
Australia	120,000+	Very Strong (WHS Act)	Crowded Places Strategy	Year 2-3
Germany	270,000	Strong (EU Directives)	EU CT Agenda	Year 3
France	180,000	Strong (Vigipirate/SILT)	Post-2015 legislation	Year 3
UAE	100,000+	Developing	Smart city investment	Year 3
Saudi Arabia	150,000+	Developing	NEOM/Vision 2030	Year 3
India	7,000,000+	Developing	Scale opportunity	Year 4+

10.2 United Kingdom: The Launch Market

The UK is the optimal launch market for several reinforcing reasons. The workforce is large enough to achieve network effects (400,000+ licensed officers) but concentrated enough geographically (London

alone accounts for a disproportionate share) to build density quickly. The regulatory environment is the strongest in the world for this category, with Martyn's Law creating a hard compliance deadline. Established relationships with SIA-approved training providers and industry distribution channels provide direct access to officers at the point of licensing. And the cultural context—a workforce that is underpaid, undervalued, and isolated—creates genuine demand for a tool that provides community and recognition.

The UK launch plan targets the following sequence:

Phase 1 (Months 1-6): London density. Focus exclusively on building network density in central London zones—Oxford Street, Regent Street, the City, Canary Wharf, Westfield centres. These areas have the highest concentration of security officers per square kilometre and the most immediate need for cross-employer communication.

Phase 2 (Months 6-12): Major cities. Expand to Manchester, Birmingham, Leeds, Glasgow, Edinburgh, Bristol, Liverpool. Target city centres and major retail/entertainment districts.

Phase 3 (Months 12-18): National coverage. Expand to all major urban areas and begin targeting specific verticals (hospitals, universities, transport hubs).

10.3 United States: The Scale Market

The United States represents the largest single market opportunity. With over 1.1 million private security guards—significantly outnumbering the approximately 666,000 sworn police officers—the workforce is massive and growing. The regulatory environment, while lacking a single federal equivalent to Martyn's Law, creates strong incentives through civil liability. Venues that fail to implement reasonable security measures face multi-million-dollar lawsuits following incidents.

The US entry strategy should target specific buyer segments:

Business Improvement Districts are the ideal entry point. US BIDs operate similarly to UK BIDs, employing "Public Safety Ambassadors" who patrol districts and serve as "eyes and ears." Major BIDs in New York (Times Square Alliance, Downtown Alliance), Los Angeles, Chicago, and Washington DC have substantial security budgets and a mandate to coordinate safety across their districts.

University campuses represent a concentrated, high-value market. There are over 4,000 degree-granting institutions in the US, most with dedicated campus security forces. The Clery Act requires universities to report campus crime statistics, creating strong incentives to adopt tools that improve safety outcomes.

Corporate campuses and commercial real estate in major cities face the same cross-tenant coordination challenges as UK shopping malls. A single office tower may have multiple security contractors serving different tenants, none of whom can communicate with each other.

10.4 The Gulf: Smart City Infrastructure

The Gulf Cooperation Council states—particularly the UAE and Saudi Arabia—represent a unique opportunity. These markets are investing billions in smart city infrastructure (NEOM in Saudi Arabia,

Masdar City in Abu Dhabi, Dubai's Smart City initiative) and require security communication networks built from scratch. Unlike mature markets where OnSiren must displace legacy systems, Gulf smart cities can adopt OnSiren as their foundational security communication layer from day one.

The cultural context is also favourable. Private security in the Gulf is a rapidly growing industry (CAGR 10.8% in the Middle East and Africa region, 2025-2030), driven by mega-events (FIFA World Cup legacy, Expo 2030), tourism expansion, and the diversification of economies away from oil dependence.

The entry strategy for the Gulf should leverage sovereign wealth fund investment (Mubadala, PIF) as both capital and distribution. A strategic investment from a Gulf sovereign fund would provide not only funding but immediate access to government decision-makers and smart city procurement processes.

10.5 Europe: Regulatory Harmonisation

The European Union's developing Protective Security Framework and Counter-Terrorism Agenda create a regulatory tailwind across all 27 member states. Germany (270,000 security workers) and France (180,000) are the priority markets, followed by the Netherlands, Spain, and Italy.

The European entry should be timed to coincide with EU-level regulatory developments, positioning OnSiren as a cross-border solution that helps multinational security companies (G4S/Allied Universal, Securitas, ISS) comply with harmonised requirements across multiple jurisdictions simultaneously.

---

12. The UK Launch Plan: Specific Targets

11.1 Business Improvement Districts (341 Active BIDs)

The UK has approximately 341 active Business Improvement Districts across England, Scotland, Wales, and Northern Ireland, with over 70 in London alone. BIDs have tripled since 2010, reflecting growing demand for coordinated local management of commercial areas. Each BID is governed by a BID Manager who controls the operational budget and procurement decisions.

OnSiren's BID strategy is straightforward: offer the app free to all workers in the BID area, and charge the BID a modest SaaS fee for the management dashboard that provides oversight, analytics, and police interface capability. The value proposition to the BID Manager is: "Replace your £30,000/year radio scheme with a free app that connects ten times more people and gives you data you've never had before."

Priority London BIDs for initial outreach include: New West End Company (Oxford Street, Bond Street, Regent Street), Heart of London Business Alliance (Piccadilly, Leicester Square), Team London Bridge, Paddington BID, Victoria BID, and Baker Street Quarter Partnership.

11.2 Police Forces (43 Territorial Forces)

England and Wales have 43 territorial police forces, plus Police Scotland and the Police Service of Northern Ireland (45 total), plus three special police forces (British Transport Police, Civil Nuclear Constabulary, Ministry of Defence Police). Total police officer strength is approximately 149,000 across England and Wales.

OnSiren's police engagement strategy should target:

Counter Terrorism Security Advisers (CTSAs): Approximately 200 CTSAs operate across the UK, each responsible for advising businesses in their force area on protective security. They are the individuals who will be asked "how do we comply with Martyn's Law?" by thousands of venues. If CTSAs recommend OnSiren as a compliance tool, adoption will follow.

National Counter Terrorism Security Office (NaCTSO): The police unit under the Home Office that manages CTSAs and publishes protective security guidance. Endorsement from NaCTSO would be transformative.

National Business Crime Centre (NBCC): The police resource for business crime prevention that has already developed data-sharing frameworks (Form A and Form B) for retail-to-police and police-to-retail information exchange. OnSiren's police interface should be designed to comply with these existing frameworks.

City of London Police: Already operates CityINTEL with the City Security Council. The City of London Police is the natural pilot partner for demonstrating how OnSiren's bottom-up data complements CityINTEL's top-down intelligence.

11.3 Key Organisations and Charities

Tier 1: Immediate Strategic Partners

ORGANISATION	ROLE	WHY PARTNER
Security Industry Authority (SIA)	Regulator	Martyn's Law enforcement body; endorsement = credibility
NaCTSO / ProtectUK	CT guidance	Publishes protective security tools and guidance
City Security Council (CSC)	Industry body	50 largest UK security companies; national reach
British Security Industry Association (BSIA)	Trade association	Members provide 70%+ of UK security by turnover
SIA-approved training providers	Training network	Direct access to officers during licensing; national distribution

Tier 2: Crime Reduction and Community Safety

ORGANISATION	ROLE	WHY PARTNER
National Business Crime Centre (NBCC)	Police resource	Data-sharing framework already established
Crimestoppers	Anonymous reporting	Complementary mission; shared intelligence
Safer Business Network	London's largest BCRP	Direct access to London retail security
DISC Platform	Digital intelligence sharing	Used by 70% of London BIDs; potential integration

Tier 3: Mental Health and Worker Welfare

ORGANISATION	ROLE	WHY PARTNER
Security Minds Matter	Mental health charity	Shared mission; co-branded welfare content
Suzy Lamplugh Trust	Lone worker safety	Pioneered the field; credibility by association
Mind	Workplace mental health	Resources for officer wellbeing

Tier 4: Community Resilience

ORGANISATION	ROLE	WHY PARTNER
Community Security Trust (CST)	Jewish community protection	3,700+ incidents/year; real-time alerting need
Tell MAMA	Anti-Muslim hate monitoring	Incident reporting; community protection
Neighbourhood Watch	Community vigilance	2.3 million households; shared philosophy
Street Pastors	Night-time economy volunteers	12,000+ volunteers; 270+ teams

---

13. The Police Interface: Why Law Enforcement Should Use OnSiren

12.1 The Intelligence Gap

UK policing faces a structural intelligence gap regarding activity on the ground in public spaces. Police forces have access to CCTV (reactive, not proactive), Airwave radio (internal only), and public reporting

channels (delayed, unstructured). What they lack is real-time, structured, verified intelligence from the thousands of trained professionals already deployed in public spaces.

Private security officers collectively observe more of the public realm than police officers do. They are present in locations and at times when police are not. They notice patterns over days and weeks that a passing patrol cannot detect. But currently, this observational intelligence has no structured pathway into police systems. It is lost—trapped in the heads of individual officers who have no mechanism to share it.

12.2 How OnSiren Interfaces with Police

OnSiren's police interface is designed to comply with the National Business Crime Centre's existing data-sharing framework. Alerts that meet defined criteria (severity level, type, verification status) are automatically formatted and transmitted to the relevant police force's intelligence system. The data is structured (type, location, time, severity, number of confirming nodes) rather than raw (unverified voice or text).

The police receive intelligence that is: - **Real-time:** Alerts arrive within seconds of generation - **Geo-located:** Precise coordinates, not vague descriptions - **Verified:** Multiple nodes confirming the same alert increases confidence - **Structured:** Machine-readable format compatible with existing police systems - **Actionable:** Clear type classification enables appropriate response grading

12.3 Project Servator Alignment

Project Servator—the police tactic using unpredictable, highly visible deployments of specially trained officers to spot hostile reconnaissance—explicitly relies on the community being "eyes and ears." The tactic has resulted in arrests, removal of firearms, knives, and drugs. But its effectiveness is limited by the absence of a persistent digital channel through which those "eyes and ears" can communicate what they observe.

OnSiren provides that channel. Security officers trained in hostile reconnaissance detection (through ACT Awareness or equivalent programmes) can report observations through the app, creating a persistent intelligence feed that complements Servator deployments. The police gain access to a distributed sensor network that operates 24/7, not just during Servator operations.

---

14. Investor Mapping

13.1 Why Invest in OnSiren

The investment thesis for OnSiren rests on five pillars:

1. **Regulatory catalyst with a hard deadline.** Martyn's Law creates mandatory demand for protective security solutions across 155,000+ UK premises by April 2027. This is not speculative demand—it is legislated.

2. **Network effects create a defensible moat.** Each additional node makes the network more valuable for every existing node. Once OnSiren achieves critical density in a zone, switching costs become prohibitive—no competitor can replicate the network without the users.
3. **Proprietary data asset.** The real-time safety data generated by the network—incident types, locations, times, patterns, response effectiveness—is unique. No government, no police force, and no CCTV network generates this data. It is the foundation of a data business worth multiples of the communication platform itself.
4. **Proven category.** Motorola Solutions acquired Rave Mobile Safety (validating institutional safety communication). Citizen App raised $133 million (validating consumer safety awareness). Zello achieved $23.5 million ARR with 20 staff (validating smartphone-based radio networks). The category is proven; OnSiren combines elements of all three into a single platform.
5. **Distribution advantage.** Direct relationships with SIA-approved training providers and industry distribution channels provide access to security officers at the point of licensing—the moment they enter the profession. This is a distribution route that no competitor can readily replicate.

13.2 UK Investors

INVESTOR	STAGE	THESIS FIT	RATIONALE
Seedcamp	Pre-seed/Seed	Network effects, European scale	Backed Revolut early; understands network-effect businesses
JamJar Investments	Seed	Consumer challenger brands	£100M fund; British Business Bank backed; mission-driven brands
Octopus Ventures	Pre-seed to Series A	Deep tech + consumer	Safety-as-infrastructure; social impact angle
Hoxton Ventures	Early stage	Network effects	Backed Deliveroo; understands gig economy adjacency
LocalGlobe / Latitude	Early stage	Community infrastructure	Backed Citymapper; city-level infrastructure plays
Amadeus Capital Partners	Seed to Series A	Security technology	Invested in Pimloc (AI security/video privacy)
Notion Capital	Series A	B2B SaaS/Cloud	€114M growth fund; British Business Bank backed
BGF (British Growth Fund)	Growth	UK scale-ups	£2.5B+ deployed; patient capital for UK businesses
NATO Innovation Fund	Growth	Defence/security deep tech	€1B+; 24 NATO allies; counter-terrorism infrastructure

13.3 US Investors

INVESTOR	STAGE	THESIS FIT	RATIONALE
a16z (American Dynamism)	Series A+	Public safety technology	$1.2B+ invested in public safety tech; "Superhero Stack" thesis
Sequoia Capital	Series A+	Network effects at scale	Invested in Citizen App; understands safety networks
Founders Fund	Early to Growth	Contrarian infrastructure	Invested in Citizen App; defence/dual-use thesis
Alumni Ventures (Strategic Tech)	Seed to Series A	Public safety, dual-use	Recent: Aslan Protects, Closure Intelligence
Responder Corp Ventures	Early stage	First responder technology	Founded BY first responders; deep domain expertise
LLR Partners	Growth	Public safety software	Mandate to "modernize public safety operations"
Paladin Capital Group	Multi-stage	Cyber and physical security	Washington DC; government/security focus
ADT Ventures	Strategic	Security infrastructure	Corporate VC; Google invested $450M in ADT; distribution potential
In-Q-Tel	Strategic	Intelligence community	CIA-linked VC; dual-use civilian/intelligence applications

13.4 Gulf and Impact Investors

INVESTOR	STAGE	THESIS FIT	RATIONALE
Mubadala (Abu Dhabi)	Growth	Smart city infrastructure	Sovereign wealth; Gulf market entry
Saudi Aramco Ventures / NEOM	Strategic	Smart city from scratch	NEOM requires entire security infrastructure
Bethnal Green Ventures	Pre-seed	Tech for good	Social impact; worker welfare
Omidyar Network	Growth	Responsible technology	Civic tech; community infrastructure
Schmidt Futures	Growth	Technology for public benefit	Infrastructure for public safety

15. SWOT Analysis

Strengths

OnSiren's primary strength is its architectural differentiation. The worker-first, bottom-up adoption model creates a network that no top-down enterprise platform can replicate. The geo-fenced channel structure breaks organisational silos in a way that employer-controlled systems cannot. The alert-first design creates a fundamentally different product category from push-to-talk apps like Zello. Established distribution relationships with the licensing and training ecosystem provide direct access to the workforce at the point of professional entry. The regulatory timing—launching 12 months before Martyn's Law compliance deadline—is optimal. The premium brand identity (tactical aesthetic, NATO callsigns, sonar interface) elevates the profession and creates emotional attachment. The free pricing for individuals eliminates all adoption barriers.

Weaknesses

The platform is pre-revenue and unproven at scale. Network effects require critical mass to deliver value—a single officer in an empty zone receives no benefit. The worker-first model means slower enterprise revenue generation compared to direct B2B sales. The reliance on smartphone connectivity means the app is dependent on mobile network coverage and battery life. The absence of a formal response capability means OnSiren cannot guarantee outcomes—it provides awareness, not intervention. Building trust with police forces and government bodies requires time, credibility, and formal security certifications that a startup may not initially possess.

Opportunities

Martyn's Law creates mandatory demand across 155,000+ premises. The global private security market exceeds $256 billion and is growing. The gig economy workforce (millions of lone workers) represents a massive adjacent market. International regulatory convergence (EU CT Agenda, Australia's Crowded Places Strategy) creates multiple market entry points. The data generated by the network has standalone commercial value for insurers, urban planners, and law enforcement. Smart city developments in the Gulf require security infrastructure from scratch. Potential strategic acquisition by Motorola Solutions, Axon, or a major security company validates the exit path.

Threats

Incumbent platforms (Zinc, Motorola MOTOTRBO) could develop competing features. Police forces could mandate a government-controlled alternative. Data privacy concerns or a high-profile false alert could damage trust. Employer resistance (attempting to ban the app) could slow adoption in some sectors. A major security incident where OnSiren is present but fails to prevent harm could generate negative publicity. Citizen App-style controversies (vigilantism, profiling) could taint the category. Funding constraints could prevent achieving critical mass before competitors respond.

16. PESTEL Analysis

Political

The political environment is highly favourable. Martyn's Law has cross-party support and is now enacted. The UK government's Protect and Prepare strategy explicitly calls for better coordination between private security and law enforcement. Counter-terrorism remains a top political priority across all major parties. The Security Industry Authority's expanded role under Martyn's Law creates a regulatory body actively seeking solutions to recommend.

Economic

The UK private security market is valued at approximately $6.81 billion (2024) and growing. Security spending by businesses is increasing in response to rising retail crime, anti-social behaviour, and the Martyn's Law compliance requirement. However, economic pressures on businesses (inflation, energy costs, wage increases) mean that cost-effective solutions are preferred over expensive hardware deployments. OnSiren's free-for-individuals model is economically aligned with a cost-constrained market.

Social

Public concern about crime, terrorism, and anti-social behaviour is elevated. The mental health crisis in the security workforce is gaining recognition (Security Minds Matter, academic research). The gig economy has normalised app-based work coordination. Younger workers expect smartphone-based tools rather than legacy hardware. The cultural shift toward community-based safety (Neighbourhood Watch revival, Street Pastors growth) creates receptivity to collective vigilance concepts.

Technological

Smartphone penetration among the security workforce is near-universal. 4G/5G coverage in urban areas is sufficient for real-time alerting. GPS accuracy on modern smartphones enables precise geo-fencing. Push notification infrastructure (Apple APNs, Google FCM) provides reliable alert delivery. AI capabilities for pattern recognition, severity classification, and predictive alerting are rapidly maturing. LiDAR and sensor technology for the OnSiren Mobile vehicle is commercially available.

Environmental

Climate change is increasing the frequency of extreme weather events that require coordinated emergency response. Urban densification is creating more crowded public spaces with higher security requirements. The shift toward 15-minute cities and mixed-use developments creates more complex security environments that require coordination across multiple stakeholders.

Legal

Martyn's Law creates mandatory compliance requirements. The Health and Safety at Work Act 1974 and Management of Health and Safety at Work Regulations 1999 impose duty-of-care obligations on employers. The Corporate Manslaughter Act 2007 creates severe penalties for safety failures. UK GDPR requires careful handling of location data but permits processing for legitimate safety interests. The Alsnih employment tribunal case supports workers' rights to use personal safety apps. The NBCC data-sharing framework provides a compliant pathway for police interface.

---

17. Measurement Framework: How We Track Success

16.1 Network Health Metrics

METRIC	DEFINITION	TARGET (YEAR 1)
Active nodes	Officers with app open in last 24 hours	80,000
Zone density	Average active nodes per geo-fenced zone	15+
Coverage hours	Percentage of time each zone has 3+ active nodes	80%+
Cross-employer connections	Percentage of zones with officers from 2+ employers	60%+

16.2 Safety Impact Metrics

METRIC	DEFINITION	TARGET
Alert response time	Time from alert to first acknowledgment by nearby node	Under 30 seconds
Alert propagation reach	Average number of nodes reached per alert	25+
Incident de-escalation rate	Percentage of alerts where situation resolved without police	Track and report
Officer welfare check compliance	Percentage of lone workers checking in on schedule	90%+

16.3 Mental Health and Wellbeing Metrics

METRIC	DEFINITION	METHOD
Perceived isolation	Self-reported feeling of being alone at work	Quarterly survey

METRIC	DEFINITION	METHOD
Peer support utilisation	Frequency of non-emergency PTT usage	App analytics
Network belonging	Self-reported sense of professional community	Quarterly survey
Stress indicators	Self-reported occupational stress levels	Annual wellbeing survey

16.4 Commercial Metrics

METRIC	DEFINITION	TARGET (YEAR 1)
User acquisition cost	Cost per activated officer	Under £2
Monthly active users	Officers using app at least once per month	60,000+
Employer dashboard subscriptions	Paid command-and-control accounts	200+
BID partnerships	Active BID management dashboard contracts	30+
Police force integrations	Forces receiving OnSiren data feed	5+

18. Data Privacy and Trust Architecture

17.1 Principles

OnSiren's trust architecture is built on five principles derived from the failures of Citizen App and the requirements of UK GDPR:

Data belongs to the user. Officers have granular control over their data, including the ability to control visibility, opt out of specific data sharing, and delete their history. Location tracking occurs only when the app is actively in use—there is no background surveillance.

Anonymisation by default. Alerts are attributed to callsigns, not real names. Officers choose how much personal information to share with the network. Incident reports flowing to the police interface are anonymised unless the officer explicitly consents to identification.

Verification before propagation. Unlike Citizen App's unvetted crowdsourced reports, OnSiren alerts are generated by verified, licensed professionals. The SIA licence verification at registration ensures that every node in the Guards layer is a trained, vetted individual.

Anti-vigilantism by design. OnSiren explicitly communicates that it is for awareness and alerting, not for intervention or pursuit. The app's messaging, onboarding, and terms of use make clear that officers should not approach threats based solely on alerts from others. The purpose is awareness, not action.

Transparency with law enforcement. The conditions under which data may be shared with police are clearly communicated to users at registration. Officers understand that high-severity alerts may be transmitted to police systems, and they consent to this as a condition of network membership. There are no hidden data flows.

17.2 UK GDPR Compliance

Under UK GDPR, location data is personal data when it can identify an individual. OnSiren processes location data under the "legitimate interests" lawful basis (Article 6(1)(f)), having conducted a Legitimate Interests Assessment that balances the safety benefits of the network against the privacy impact on users. Data minimisation principles are strictly applied: location is processed only during active app use, stored only as long as necessary for network function, and anonymised in all aggregate analytics.

The ICO's guidance on sharing personal data with law enforcement authorities confirms that UK GDPR does not prevent sharing where it is necessary and proportionate for the prevention or detection of crime. OnSiren's police interface operates within this framework, sharing structured alert data (not raw location tracking) under the "crime and taxation" exemption in Schedule 2 of the Data Protection Act 2018.

---

19. Vision: What OnSiren Is

OnSiren is not a security company. It does not employ guards. It does not respond to incidents. It does not replace police, emergency services, or employer-mandated safety systems.

OnSiren is digital infrastructure. It is the connective tissue between the people who already stand watch. It takes the half-million trained professionals who are already deployed into the physical world every day—and the millions more who work on the frontline of public life—and gives them what they have never had: the ability to hear each other.

The vision is simple and ancient. Human beings have always survived by sharing information about threats. From the tribal watchfire to the medieval Hue and Cry to the town crier to the neighbourhood watch, the architecture has always been the same: immediate, peer-to-peer communication of threat information within a defined geographic area. OnSiren is this architecture, digitised for the smartphone era.

The network has two layers. The Guards—licensed security professionals who are trained to respond—form the verified backbone. The Watchers—shopkeepers, drivers, transport workers, hospitality staff—extend the network into every street, every vehicle, every counter. Together, they form a living sensor network that generates real-time safety intelligence no government, no police force, and no CCTV system can replicate.

The data this network generates is the real asset. Every alert, every acknowledgment, every propagation event, every welfare check is a data point. At scale, this data reveals the safety state of every street in a city, in real-time, 24 hours a day. It reveals patterns that no other system can detect. It

enables prediction that no other dataset can support. It is, ultimately, the foundation of a new category: civilian safety intelligence.

OnSiren exists because the isolation of frontline workers is unacceptable. Because a security officer finishing a 12-hour night shift should not have to process their fear alone. Because a shopkeeper who notices something wrong should be able to tell someone instantly. Because a delivery rider being followed through a dark street should know that other riders are nearby. Because the people who keep everyone else safe deserve to be connected to each other.

The siren is the oldest alarm in human civilisation. OnSiren is its digital descendant.

References

1. Sampson, R.J., Raudenbush, S.W., and Earls, F. (1997). "Neighborhoods and Violent Crime: A Multilevel Study of Collective Efficacy." *Science*, 277(5328), pp. 918-924.
2. Bandura, A. (1982). "Self-efficacy mechanism in human agency." *American Psychologist*, 37(2), pp. 122-147.
3. Dunbar, R.I.M. (1998). "The Social Brain Hypothesis." *Evolutionary Anthropology*, 6(5), pp. 178-190.
4. Jacobs, J. (1961). *The Death and Life of Great American Cities*. New York: Random House.
5. National Institute of Justice (2016). "Collective Efficacy: Taking Action to Improve Neighborhoods." US Department of Justice.
6. Hipp, J.R. (2016). "Collective efficacy: How is it conceptualized, how is it measured, and does it really matter for understanding perceived neighborhood crime and disorder?" *Journal of Criminal Justice*, 46, pp. 32-44.
7. Talas, A., Button, M., Doyle, M., and Das, J. (2021). "Violence, abuse and the implications for mental health and wellbeing of security operatives in the United Kingdom: the invisible problem." *Policing and Society*, 31(8), pp. 964-981.
8. British Security Industry Association (2024). *Annual Industry Report*. London: BSIA.
9. Cogan, N. (2026). "Persistent Traumatic Stress Exposure: Rethinking PTSD for Frontline Workers." *Healthcare*, 14(2).
10. Shalaby, R.A.H. and Agyapong, V.I.O. (2020). "Peer Support in Mental Health: Literature Review." *JMIR Mental Health*, 7(6), e15572.
11. Health and Safety Executive (2024). "Lone working: Protect those working alone." HSE Guidance. Available at: https://www.hse.gov.uk/lone-working/
12. Canadian Centre for Occupational Health and Safety (2023). "Working Alone: Health and Safety Guide." CCOHS.

13. Security Industry Authority (2025). "Annual Report and Accounts 2024-25." London: SIA.

14. UK Government (2025). *Terrorism (Protection of Premises) Act 2025*. London: HMSO.

15. UK Government (2025). "Terrorism (Protection of Premises) Act 2025: Statutory Guidance." Home Office.

16. Alsnih v. Al Quds Al-Arabi Publishing & Advertising. Employment Tribunal. Cited in Littler (2023).

17. Health and Safety at Work etc. Act 1974, Section 2. Legislation.gov.uk.

18. Management of Health and Safety at Work Regulations 1999. Legislation.gov.uk.

19. Corporate Manslaughter and Corporate Homicide Act 2007. Legislation.gov.uk.

20. BS 8484:2022. "Provision of lone worker services: Code of practice." British Standards Institution.

21. National Business Crime Centre (2024). "Retail Data Sharing Process." NBCC/NPCC.

22. City of London Police (2004). "Project Griffin." CoLP.

23. NaCTSO (2024). "ProtectUK Guidance." National Counter Terrorism Security Office.

24. British BIDs (2024). "BID Data Report." British BIDs.

25. Rocket Science (2024). "BIDs in the UK: Landscape Report." Commissioned by MHCLG.

26. HMICFRS (2025). "Police Forces in England and Wales." His Majesty's Inspectorate of Constabulary.

27. Grand View Research (2025). "Private Security Services Market Size Report, 2030."

28. Future Market Insights (2025). "Private Security Market: Global Analysis Report."

29. AGC Partners (2025). "Physical Security Technology Investment Report."

30. Electronic Frontier Foundation (2021). "Crowd-Sourced Suspicion Apps Are Out of Control." EFF Deeplinks.

31. Reforge (2024). "Zello: Growth and Monetization Analysis." Reforge Blog.

32. Information Commissioner's Office (2024). "Legitimate Interests Guidance." ICO.

33. Information Commissioner's Office (2024). "Sharing Personal Data with Law Enforcement Authorities." ICO.

34. Motorola Solutions (2022). "Motorola Solutions Completes Acquisition of Rave Mobile Safety." Press Release.

35. RapidSOS (2024). "Uber Case Study: Connected Safety." RapidSOS.

36. Community Security Trust (2025). "Antisemitic Incidents Report 2025." CST.

37. Security Minds Matter (2024). "About Us." Available at: https://securitymindsmatter.org/

38. Suzy Lamplugh Trust (2024). "Personal Safety at Work." Available at: https://www.suzylamplugh.org/

39. Australia's Strategy for Protecting Crowded Places from Terrorism (2024 Update). Australian Government.

40. EU Counter-Terrorism Agenda (2020). European Commission.

This white paper was produced through desktop-based research using publicly available academic publications, government documents, industry reports, and credible media sources. All citations refer to verifiable sources. The research was commissioned by OnSiren Limited to inform strategic decision-making and stakeholder engagement.