QUARTERLY NEWSLETTER

PREPARED BY: PERALTA ASSOCIATES
Peralta Management Co Llc

Experience Breakdown

71.2%
of roles required adaptability, communication, and decision making abilities.

Systemic Analyze & Report Findings

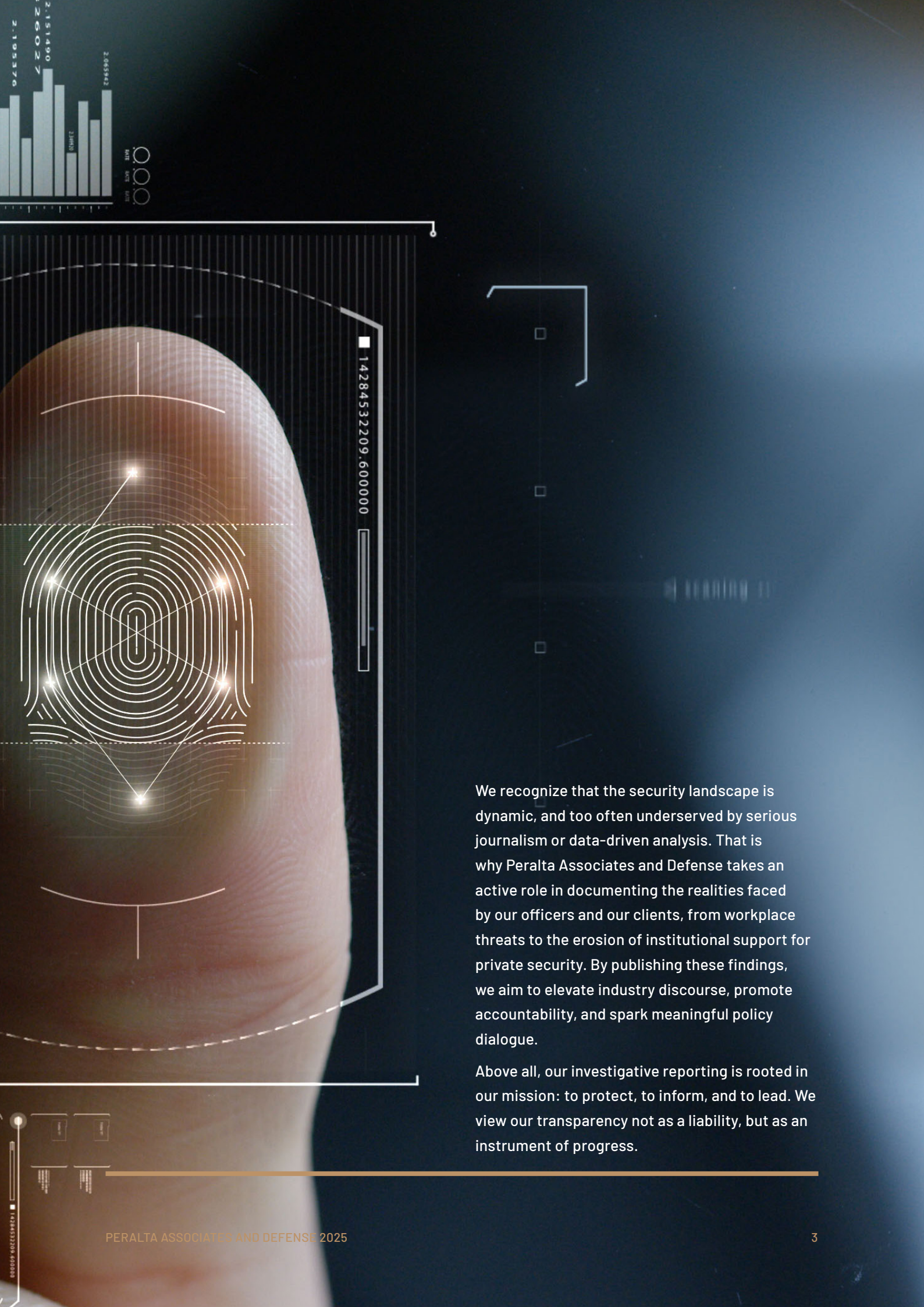
PERALTA
ASSOCIATES & DEFENSE

INVESTIGATIVE REPORTING

At Peralta Associates and Defense, we believe that knowledge is not only power, it is a professional obligation. Our commitment to investigative excellence extends beyond serving clients in the field; it includes informing, educating, and advancing the standards of the private security and investigations industry as a whole.

Through our investigative reporting initiatives, we bring to light critical issues that impact private security professionals, law enforcement, and public safety stakeholders. Whether it's uncovering systemic challenges in officer accountability, analyzing the evolving role of surveillance technologies, or exploring the implications of legislative gaps that affect frontline security workers, our reports are grounded in first-hand operational experience, factual data, and verified field intelligence.

Our reporting process is rigorous and responsible. We combine open-source intelligence (OSINT), field interviews, legal research, and on-the-ground observations to produce actionable insights. These findings are not only shared internally for continuous training and operational improvement but are also published through professional channels to foster awareness and advocacy throughout the industry.



We recognize that the security landscape is dynamic, and too often underserved by serious journalism or data-driven analysis. That is why Peralta Associates and Defense takes an active role in documenting the realities faced by our officers and our clients, from workplace threats to the erosion of institutional support for private security. By publishing these findings, we aim to elevate industry discourse, promote accountability, and spark meaningful policy dialogue.

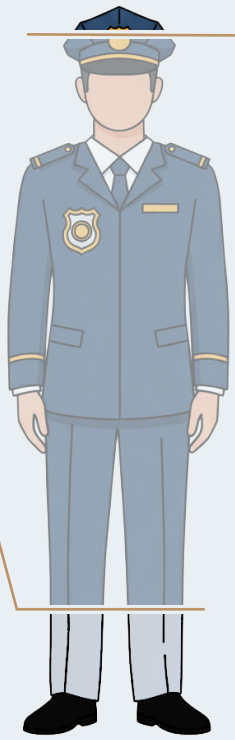
Above all, our investigative reporting is rooted in our mission: to protect, to inform, and to lead. We view our transparency not as a liability, but as an instrument of progress.

WHY THE QUALITY OF SECURITY SERVICES IS IN DECLINE

In today's increasingly complex and unpredictable environment, safety, risk management, and operational continuity have become top priorities across all sectors from retail and commercial real estate to logistics, healthcare, and critical infrastructure. As traditional law enforcement resources become more strained, private security services have stepped in to fill the gap, providing frontline protection for businesses, public institutions, and communities.

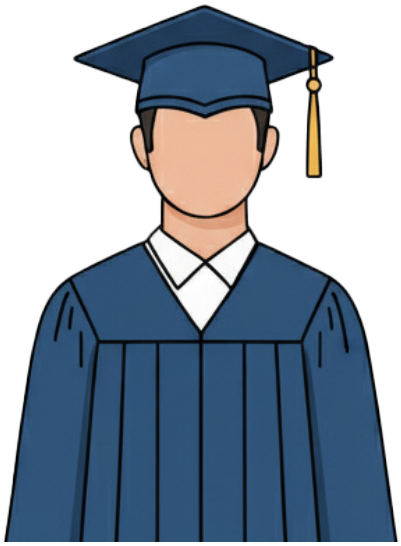
Despite this growing reliance, however, the overall quality of private security services has been steadily declining. What should be a professional, disciplined, and highly trained workforce is too often seen delivering inconsistent performance, inadequate deterrence, and in some cases, contributing to reputational and legal liabilities for the organizations they're meant to protect. This deterioration has not gone unnoticed it has raised red flags among clients, law enforcement, and industry insiders alike.

EXPERIENCE BREAKDOWN



99.5% of security guards completed on-the-job training, underscoring that experience is overwhelmingly acquired during employment

In 2024, only **10.9%** of security guards were required to have prior work experience, meaning nearly **89%** **entered the field without** previous security background.



EDUCATION

A high school diploma (or equivalent) is required for **73.8%** of security guard roles.

Employers increasingly value cognitive skills: in 2024, **71.2%** of roles required adaptability, communication, and decision-making abilities

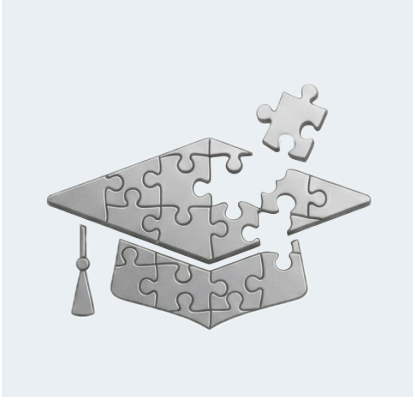
SYSTEMIC BREAKDOWNS

This decline is not the result of a single issue, but rather a systemic breakdown across several key areas: underinvestment in training, low industry wages, high turnover, minimal regulatory oversight, and a profit-first mentality that sacrifices long-term value for short-term gain. In many regions, the industry has shifted from being a trusted security solution to little more than a "warm-body service" focused on post coverage, not performance.

The consequences are far-reaching. Vulnerabilities are left unaddressed. Threats go undetected. Incidents escalate due to poor situational awareness and lack of de-escalation training. And clients, many of whom entrust security firms with safeguarding millions in assets and human lives, are left under-protected and overexposed.

This article examines the underlying causes of the decline in service quality, the operational and ethical risks it presents, and most importantly, what must be done to restore professionalism, accountability, and trust in the security industry. It is not simply a critique—it is a call to action for providers, clients, and regulators to reimagine private security as a strategic, skill-based profession rather than a cost-centered commodity.

Now more than ever, reform is not optional, it's essential. The safety of people, property, and mission-critical operations depends on it.



INADEQUATE TRAINING

At the core of any high-performing security operation is robust, continuous training. Yet, in much of the private security industry, training is viewed not as a critical investment but as a regulatory formality—a checkbox to meet minimum legal requirements.

In many states, becoming a licensed security officer requires little more than 8 to 40 hours of generalized instruction. These courses often focus on liability avoidance, basic patrol procedures, or outdated emergency protocols, and fail to address the real-world demands of the role. Officers are frequently placed in high-risk or high-traffic environments with no site-specific orientation, limited conflict de-escalation training, and little to no exposure to active threat response, customer engagement, or report writing.

JUDGMENT

Judgment-based decision-making; teaching officers to assess situations, weigh potential outcomes, and apply the most appropriate course of action within the scope of legal and ethical boundaries.

LEADERSHIP

Communication and de-escalation; developing the interpersonal skills needed to resolve conflicts peacefully, gain compliance, and defuse tense encounters.

GROWTH

Tactical readiness; preparing officers to respond effectively and decisively in high-stress situations.

Even worse, continuing education is rarely emphasized or enforced. While threats continue to evolve cybersecurity risks, active shooter scenarios, workplace violence, and insider threats many officers remain ill-equipped to respond with confidence or competence.

To reverse the decline in service quality, the security industry must shift away from checkbox training models and embrace scenario-based, continuous learning as a core pillar of professional development. A static, one-time training session is no longer sufficient in an evolving threat landscape where security officers are expected to act not just as observers, but as first responders, customer service ambassadors, and crisis managers. Scenario-based training replicates real-world situations in a controlled environment, allowing officers to practice and refine their skills in high-pressure, consequence-driven simulations. Whether responding to an aggressive individual, identifying suspicious behavior, managing access control under duress, or handling a medical emergency, these scenarios are designed to build muscle memory, critical thinking, and confidence.

HIGH TURNOVER

Few industries suffer from employee turnover at the scale seen in private security. National averages range between 100% and 300% annually, meaning some firms replace their entire workforce multiple times per year.

> "The root causes of turnover are clear: low wages, limited career progression, poor leadership, and lack of recognition.

Many officers earn just above minimum wage despite working long hours, handling unpredictable situations, and bearing significant liability. Without a clear path to advancement or professional growth, employees see the role as temporary a stepping stone, not a profession.

High turnover also undermines client trust. Frequent personnel changes lead to inconsistent service delivery, missed post responsibilities, and weakened relationships with site management.

This instability creates a number of critical problems:

- Loss of institutional knowledge
- Lack of familiarity with client sites and procedures
- Constant re-training costs

To combat this, security providers must restructure their internal culture. Competitive pay, clear promotion paths, recognition programs, and investment in professional development are all necessary to attract and retain talent. More importantly, organizations need to treat security as a career, not a placeholder.

WEAK REGULATORY OVERSIGHT

While the private security industry is regulated in most states, enforcement is often inconsistent and weak. Some states lack meaningful oversight, allowing companies with questionable practices to operate with little consequence. Licensing standards vary widely, and in some regions, the regulatory bodies are underfunded or overburdened. This regulatory gap creates an environment where mediocrity becomes normalized, and poor service goes unchecked.

Unlike public law enforcement agencies, which are governed by strict standards and accountability mechanisms, the private security industry operates under fragmented and inconsistent regulatory frameworks that vary dramatically by jurisdiction.

When we look at data from the Bureau of Labor and Statistics, a work force similar in size to security officers and their risk levels associated within that industry, training is often overlooked for security officers because of the lack of regulation and standardization.

	REQUIRED TRAINING	RISK LEVEL	2024 LABOR
SECURITY OFFICERS	8 HOURS	MODERATE-HIGH	533,000
ELECTRICIANS	4 YEARS	HIGH	810,000
LICENSED PRACTICAL NURSE	1.5 YEARS	MODERATE-HIGH	655,000

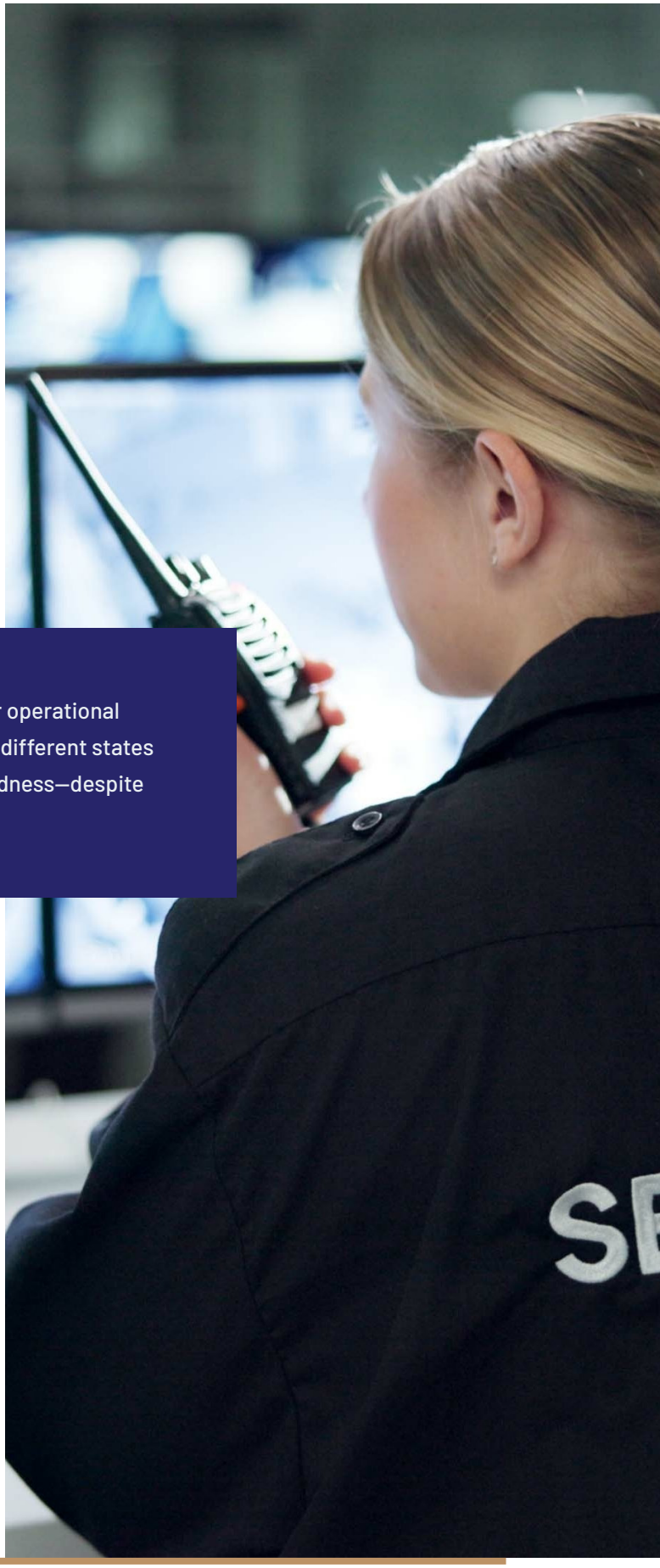
Some states maintain robust training requirements, licensing procedures, and enforcement bodies. Others offer little more than a registration database and periodic renewals. In many areas, there is no routine auditing of training programs, no enforcement of post standards, and minimal disciplinary action against underperforming firms.

This lack of oversight leads to:

- Unqualified personnel operating in sensitive environments
- Firms with poor performance histories continuing to win contracts
- Clients assuming they are protected, when in fact they are exposed

Additionally, without a national standard for training or operational benchmarks, security officers working side-by-side in different states or regions can vary significantly in quality and preparedness—despite performing identical functions.

The industry must push for stronger licensing requirements, standardized training frameworks, and active oversight at both the state and federal levels. Just as EMS, firefighting, and law enforcement are regulated to ensure competence and public trust, private security must be held to similar professional standards if it is to be seen as a credible protective force.



EASY BARRIERS TO ENTRY AND CHASING MONEY

The private security industry plays a vital role in safeguarding critical infrastructure, commercial assets, public venues, and human life. Yet, one of the most significant contributors to the erosion of service quality within the industry is the alarmingly low entry standards for security personnel. In many states and jurisdictions, the requirements to become a licensed security guard are so minimal that they fail to establish even a basic foundation of competency, professionalism, or readiness for real-world threats.

In several states, the process to become a licensed security guard can take as little as a few hours of online coursework and a background check. There are often no physical fitness requirements, no psychological screening, and no assessment on judgment, communication skills, or emotional intelligence all of which are critical in high-pressure security roles.

LOW ENTRY BARRIERS HAS SERIOUS

- Increased Risk to Clients/Public: Deploying underqualified security personnel in sensitive environments significantly increases the risk of procedural failures, delayed responses, or misuse of force, exposing clients to legal liability, reputational harm, and financial loss.
- Negative Public Perception: Unprofessional conduct by security officers undermines public trust, damages the organization's reputation, and fuels a cycle where clients prioritize cost over quality, further eroding the credibility of private security.

NEGATIVE CONSEQUENCES

- High Turnover and Low Morale: High turnover and low morale stem from a lack of professional development and employee value, leading to a revolving door of undertrained staff. This forces companies to focus more on constant recruitment than on building a skilled, accountable workforce.

This low threshold to entry has created a perception sometimes rightly so that anyone can become a security officer regardless of aptitude, attitude, or intent. It erodes public trust and discourages talented individuals from pursuing security as a legitimate, long-term career.

The reasons behind low entry standards are rooted in market demand, industry competition, and minimal regulation. Security companies, particularly those bidding on large contracts, are under pressure to staff positions quickly and affordably. To meet contractual obligations and keep costs low, some firms prioritize speed over suitability, onboarding anyone who meets the bare legal minimum.

Moreover, the lack of national licensing standards exacerbates the issue. Each state has its own licensing body, with varying levels of oversight. While some states mandate robust training and conduct field audits, others have no practical enforcement mechanisms, allowing substandard firms and unqualified guards to operate unchecked.

Without a unified standard, the industry lacks consistency in qualifications, expectations, and performance. An individual deemed unfit in one jurisdiction could legally be hired in another within days with no continuity in vetting, training, or accountability.

To elevate the industry and reverse this trend, raising entry standards must be the foundation of reform. This includes:

- **Mandatory comprehensive training** before deployment, including scenario-based exercises, ethics, and communication skills
- **Psychological and behavioral screening** to identify temperament suitability
- **National baseline licensing standards**, with room for state-specific enhancements
- **Certification and credentialing pathways** for specialized roles (e.g., hospital security, critical infrastructure protection, executive protection)
- **Mentorship and probationary periods** under senior supervision for all new officers

Most importantly, security firms must shift their mindset from merely "filling posts" to building professionals. The industry must begin to see officers not as interchangeable labor, but as frontline ambassadors and critical protectors of life, property, and reputation.

PROFITS OVER PROFESSIONALISM

One of the most damaging trends affecting the modern security industry is the prioritization of profit margins over professional standards. As demand for private security services has surged spurred by rising crime, shrinking law enforcement resources, and the need to protect critical infrastructure, many security companies have chosen to compete on price rather than value. This approach has led to a systemic erosion of service quality, undermining the industry's credibility and placing clients at greater risk.

At the heart of the issue is the contract bidding process, which often incentivizes companies to undercut one another to win contracts. In order to meet these low bids, many firms are forced to slash operational costs often at the expense of critical components such as recruitment, training, supervision, and employee benefits. The result is a workforce that is undertrained, undervalued, and unprepared to meet the real-world demands of modern security operations.

This model transforms security from a strategic safety function into a transactional, post-filling service. Guards are deployed not based on suitability, expertise, or professionalism, but simply to fill hours on a schedule. In this environment, security officers are often viewed as a cost center rather than a core element of risk management. As a consequence, incidents that could have been prevented ranging from unauthorized access and theft to workplace violence and public altercations are allowed to escalate due to lack of preparedness or oversight.

Moreover, firms that prioritize profit over professionalism tend to have high turnover rates and a reactive, rather than proactive, culture. They neglect continued training, fail to invest in leadership development, and often lack meaningful mechanisms for accountability or performance management. This results in a diluted security presence, minimal site engagement, and widespread inconsistencies in service delivery.

> "Clients, especially those unfamiliar with the nuances of private security, may not realize the hidden costs of choosing a "low bid" provider until it's too late when an incident occurs, liability increases, or a reputation is damaged. Over time, this devalues the entire industry, making it harder for reputable firms to justify fair wages, invest in training, or attract and retain top talent.

Low-margin warning signs are a clear indicator of deeper issues within the security services industry. One of the most telling signs is high employee turnover, which not only inflates recruitment and training costs but also disrupts service quality and client confidence. When companies are constantly cycling through personnel, it's nearly impossible to build a stable, professional security force. Compounding this challenge are low billing rates, often the result of aggressive underbidding. While it may win short-term contracts, this race to the bottom frequently pushes profit margins below the sustainable 5% threshold, creating financial instability that limits growth, innovation, and investment in training or technology.

The pressure to stay competitive in such a crowded marketplace often drives smaller firms to operate at break-even, or even at a loss, just to maintain their presence. This practice is not only unsustainable but detrimental to the industry's credibility. Clients may unknowingly sacrifice quality, oversight, and risk management in exchange for marginal savings, while security providers struggle to maintain compliance, morale, and service standards. Ultimately, these warning signs point to an urgent need for providers to rethink their pricing models, invest in workforce retention, and educate clients on the true cost of effective protection.

LABOR COST

Guard wages typically account for 65% to 85% of total expenses. High-wage states (e.g., CA, NY) reduce margins significantly unless pricing is adjusted accordingly.

CONTRACTS

Unarmed standing guard contracts: lower margins (~5–7%) Armed, specialized, or executive protection: higher margins (10–15%+)

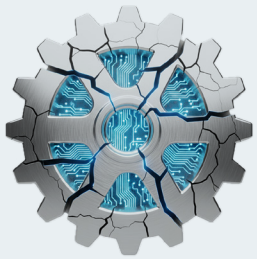
CLIENTS

Government and institutional clients may demand lower rates but longer-term contracts. Private sector clients often allow higher pricing for value-added services.

MARGIN TYPE	AVERAGE RANGE	RISK LEVEL	FACTORS AFFECTING MARGINS
NET PROFIT MARGINS	5%-10%	MODERATE-HIGH	LABOR

The path forward requires a fundamental shift in how security services are perceived and procured. Security companies must embrace professionalism, integrity, and long-term value creation as their core offerings not just manpower at the lowest possible cost. Clients, in turn, must recognize that effective security is not a commodity it's an investment in protection, continuity, and peace of mind.

By restoring professionalism as the foundation of the industry, and aligning profitability with quality, the private security sector can begin to rebuild trust, raise standards, and fulfill its critical role in today's risk-conscious world.



FAILURE TO EMBRACE TECHNOLOGY

Over the past decade, the nature and complexity of security threats have evolved at an unprecedented rate. What was once a profession primarily concerned with unauthorized access, petty theft, and loitering has now become a front-line defense against a wide spectrum of high-risk, multi-dimensional threats.

In this increasingly complex environment, the traditional approach of deploying static guards and relying on handwritten logs or radio communications is no longer adequate. Security is no longer about presence alone, it is about precision, adaptability, and foresight.

Intelligence-led security operations represent a fundamental shift in how threats are addressed and mitigated. Rather than simply reacting to incidents after they occur, this model is grounded in data collection, predictive analytics, real-time monitoring, and risk-based resource allocation. It transforms security from a passive safeguard to a dynamic, strategic function within the

THREATS

- Cyber-physical attacks that blend digital and physical intrusions to disrupt operations or access sensitive systems
- Insider threats, where employees or contractors intentionally compromise security protocols
- Workplace violence and active shooter incidents, often requiring real-time response and immediate decision-making
- Critical infrastructure vulnerabilities, especially in sectors such as utilities, data centers, healthcare, and logistics

INTELLIGENCE LED SECURITY

- Real-time situational awareness, through integrated camera systems, access control, motion sensors, and smart alarms
- Predictive analytics, utilizing historical data to anticipate high-risk times, behaviors, and patterns of criminal activity
- Centralized reporting platforms, allowing for immediate documentation, trend analysis, and response coordination
- Threat intelligence feeds, geo-fencing alerts, and interagency information sharing to track and respond to emerging threats

Organizations that integrate these tools into their daily security operations gain a tactical advantage they can prevent, not just respond to, critical incidents. They can verify compliance, audit response times, track patterns, and hold teams accountable to performance benchmarks.

Despite the clear benefits, a large portion of the private security industry remains rooted in legacy models that focus on manpower over methodology. For many firms, the approach to security has not fundamentally changed in decades: place a guard at a post, complete shift logs, patrol on foot, and wait for something to happen. Technology, if present, is often limited to outdated CCTV systems, unreliable radios, and poorly maintained access control hardware. This stagnation leads to several critical shortcomings, to include delayed or ineffective responses to missed opportunities for prevention and will reduce confidence from clients.

For security firms to remain competitive and relevant, embracing intelligence-led models is not optional it is a strategic imperative. Clients, especially in sectors like healthcare, finance, logistics, and critical infrastructure, are no longer satisfied with simple post coverage. They want providers who can offer operational visibility, incident prevention strategies, regulatory compliance reporting, integrated command and control systems, and technology that scalable.

Firms that lead this transformation will position themselves as true risk management partners, not just vendors. Those that fail to evolve will fall further behind, unable to meet client expectations or deliver meaningful value in a security landscape that is anything but predictable.

In a world where the next threat may come from a hacker, an insider, a violent intruder, or a coordinated criminal network, the security industry must respond with tools, talent, and tactics fit for today's reality not yesterday's.

> "Staying competitive requires security companies to utilize technology to their fullest extent.

CLIENT EXPECTATIONS OUTPACING PROVIDER CAPABILITIES

In today's competitive and increasingly complex security landscape, clients particularly those in high-stakes industries such as technology, logistics, healthcare, and critical infrastructure are raising their expectations. They are no longer looking for basic post coverage or uniformed presence alone; they want security partners who are technologically advanced, data-driven, and capable of delivering measurable results.

Modern organizations operate in fast-paced, risk-sensitive environments. A healthcare facility, for instance, must protect patients, staff, pharmaceuticals, and highly regulated data under HIPAA. A logistics hub faces constant vulnerability to cargo theft, supply chain disruption, and insider threats. A tech company must safeguard intellectual property, data centers, and personnel while navigating the ever-evolving landscape of cyber-physical threats. These environments require more than traditional patrol models they demand adaptive, intelligence-led security services powered by real-time information, automation, and analytical insight.

Clients in these sectors expect their providers to integrate with their systems, respond in real time, and supply analytics that inform broader organizational risk strategies. They look for automated reporting platforms, access to centralized dashboards, GPS tracking, mobile incident response apps, and security personnel trained in both physical and behavioral threat detection. In essence, they want a security provider who functions like a modern business unit not a manual labor subcontractor.

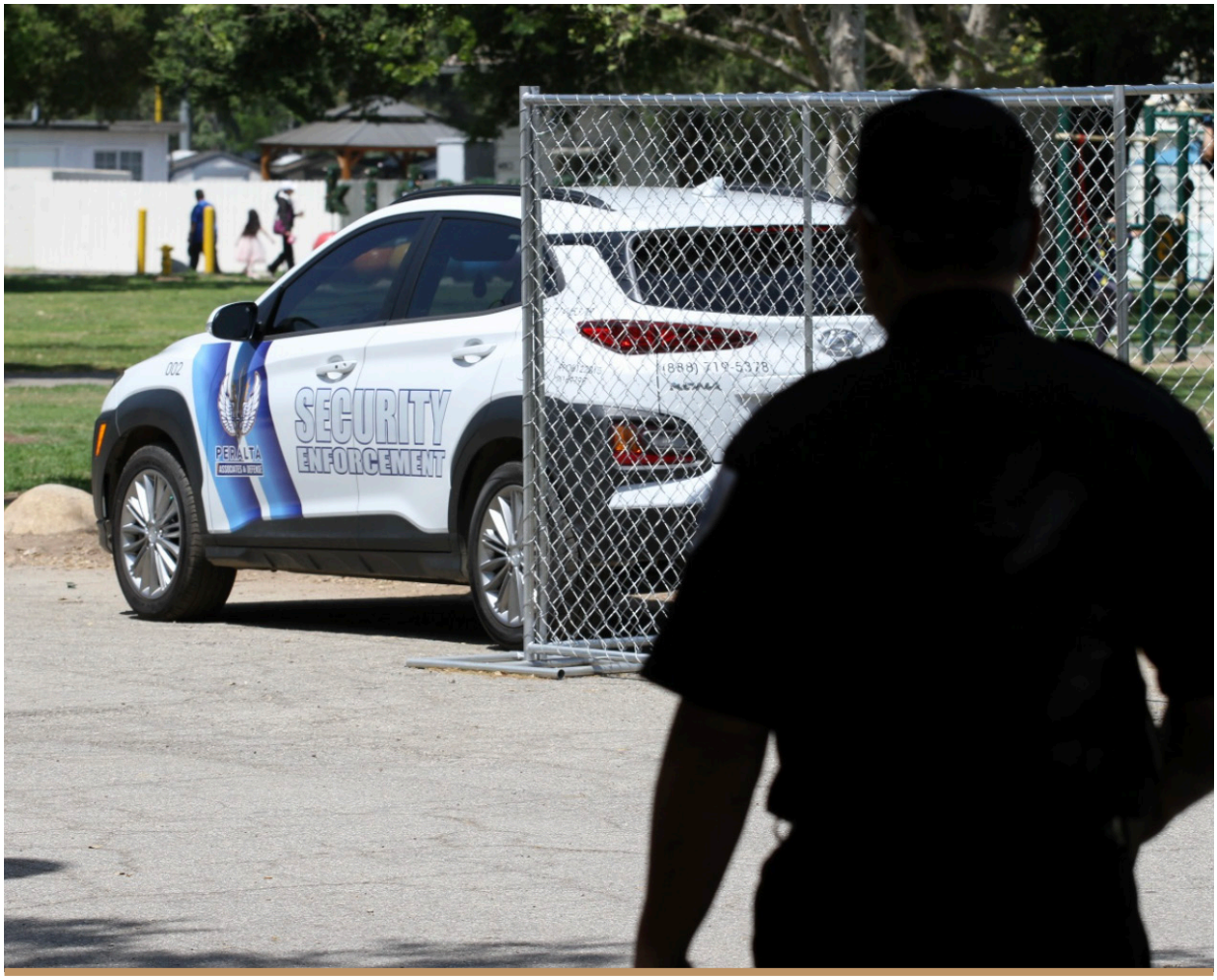
When providers lag behind in these areas, the deficiencies become quickly apparent. Poor documentation leads to unreliable incident reporting, reducing the client's ability to evaluate trends or implement corrective actions. Slow communication hinders response time, damages confidence, and can compromise emergency protocols.

Inconsistent service quality—fueled by poor supervision, limited training, or outdated processes results in missed patrols, procedural errors, and elevated liability exposure.

Clients today are more informed, connected, and data-oriented than ever before. They will notice a lack of innovation. They will notice when incidents are handwritten in a logbook instead of entered into a searchable digital platform. They will question why they cannot receive weekly incident summaries, video clips, or compliance dashboards. And when they see a provider is not evolving alongside their organization's needs, they will look elsewhere.

This disconnect doesn't just lead to minor dissatisfaction, it directly influences contract renewals, damages reputations, and erodes long-standing partnerships. In high-risk sectors, failure to modernize security services can be a deal-breaker. Clients will replace underperforming vendors with more agile, forward-thinking competitors or opt to build internal security capabilities that are more tightly integrated into their operational and IT ecosystems.

The message is clear: clients expect more because the risk environment demands more. Security providers who ignore this reality will find themselves increasingly irrelevant in a market that is rapidly moving toward integration, intelligence, and performance-based outcomes. Those who meet and exceed these expectations, however, will define the next generation of security leadership.



REPORT FINDINGS

The private security industry stands at a critical crossroads. As organizations across sectors such as technology, healthcare, logistics, and critical infrastructure increasingly rely on security firms to safeguard their assets, people, and operations, the expectations placed on the industry have never been higher. Unfortunately, many providers continue to fall short relying on outdated models, minimal training, and reactive service delivery. The result is a systemic decline in service quality, growing client dissatisfaction, and a widening gap between the security challenges of today and the tools being used to address them.

At the root of this decline are several persistent industry shortcomings: low entry standards, high employee turnover, weak regulatory oversight, underinvestment in technology, and the failure to adopt intelligence-led security operations. Many companies continue to rely on static guard deployments, paper-based reporting, and minimal supervisory oversight, approaches that are no longer sufficient in a world of complex, rapidly evolving threats. Logs go unanalyzed, incidents are treated in isolation, and data, though increasingly collected, is rarely translated into actionable insight.

The modern security client demands more. They expect data-driven decision-making, real- time visibility, measurable outcomes, and accountability at every level. Security providers who fail to embrace cloud surveillance, predictive analytics, mobile integration, and scenario-based training are rapidly being replaced by firms that do. In many cases, clients are choosing to build in-house security teams that offer more control, better integration, and higher standards of professionalism

To remain competitive, the industry must reimagine itself not as a stopgap or static service, but as a critical, intelligence-enabled function within the operational ecosystem. This transformation requires more than adopting new tools; it requires a shift in culture and leadership. Security firms must prioritize professional development, invest in strategic technologies, and implement intelligence-led frameworks that drive performance and value.

The path forward is clear. Companies that raise their standards, operationalize data, and deliver proactive, measurable security solutions will not only survive but lead the industry into its next chapter. Those that cling to outdated practices and cost-cutting measures will continue to lose relevance, contracts, and credibility.

The future of private security belongs to those willing to adapt, innovate, and lead with purpose. In an environment where threats are increasingly sophisticated and reputational stakes are high, professionalism, accountability, and intelligence are no longer optional, they are imperative.

PERALTA ASSOCIATES AND DEFENSE INVESTIGATIVE REPORTING Q3 2025

This investigative report represents the culmination of extensive research, data analysis, and firsthand interviews conducted with security industry professionals across the United States. Drawing on both quantitative and qualitative methodologies, the report integrates statistical data from reputable sources, including the U.S. Bureau of Labor Statistics, to provide a comprehensive overview of current trends, challenges, and workforce dynamics within the private security sector.

Peralta Associates and Defense dedicated nearly 300 hours to this investigation, engaging in in-depth interviews with security company executives, frontline officers, training professionals, and industry analysts. The findings reflect a rigorous commitment to uncovering the realities faced by security personnel, as well as the operational and regulatory pressures impacting the industry at large. This report aims to inform stakeholders, elevate standards, and support meaningful reform in the delivery and perception of private security services.

REFERENCES

1. ASIS International. (2022). Private Security Officer Selection and Training Guidelines (PSO-2019). Retrieved from https://www.asisonline.org
   – Provides industry standards on training, professional conduct, and screening practices.
2. U.S. Bureau of Labor Statistics (BLS). (2023). Occupational Outlook Handbook: Security Guards. Retrieved from https://www.bls.gov/ooh/protective-service/security-guards.htm
   – Includes employment statistics, wage data, and educational/training requirements in the security industry.
3. The National Association of Security Companies (NASCO). (2021). Private Security Officer Employment and Training Standards. Retrieved from https://www.nasco.org
   – Details the inconsistency of state regulations and minimum licensing standards across the United States.
4. Allied Universal. (2023). The Future of Security: Integrating Technology and Physical Security. Retrieved from https://www.aus.com
   – Explores the integration of AI, analytics, and cloud surveillance in private security operations.
5. IFSEC Global. (2022). Why Intelligence-Led Security is a Game-Changer. Retrieved from https://www.ifsecglobal.com
   – Discusses the role of predictive analytics and intelligence-driven security models in modern operations.
6. Security Industry Association (SIA). (2023). 2023 Security Megatrends Report. Retrieved from https://www.securityindustry.org
   – Covers top trends such as AI, integrated systems, and the demand for data-driven services.
7. Harvard Business Review. (2019). Why Companies Need Data-Driven Security Strategies. Retrieved from https://hbr.org
   – Supports the argument for security performance tied to measurable metrics and analysis.
8. Forbes Technology Council. (2022). Predictive Analytics in Security and Risk Management. Retrieved from https://www.forbes.com
   – Examines how businesses use historical data and AI for threat forecasting and resource optimization.
9. Gartner Research. (2023). Strategic Guide to Physical Security Technologies. Available via subscription at https://www.gartner.com
   – Provides insight on how cloud-based surveillance, mobile patrol apps, and integration platforms support next-gen security operations.
10. Department of Homeland Security (DHS). (2023). Critical Infrastructure Threats and Security Guidelines. Retrieved from https://www.cisa.gov
    – Emphasizes the importance of intelligence-led, multi-layered protection strategies for high-risk sectors.

Peralta Associates and Defense is a nationally recognized provider of comprehensive private security, investigative services, fire watch, event security, vehicle patrol, executive protection, and professional training solutions. Operating across multiple sectors and jurisdictions, we are committed to delivering excellence through innovation, discipline, and intelligence-driven strategies.

Our organization embraces the forefront of technological advancement, integrating artificial intelligence (AI), learning management systems (LMS), and automation tools to enhance service delivery, accountability, and operational efficiency. Our security teams are equipped to deploy advanced solutions, including access control systems, 24/7 remote camera monitoring, surveillance infrastructure, and other high-performance technologies designed to protect personnel, property, and sensitive assets.

In the investigative space, Peralta Associates and Defense leverages a robust ecosystem of intelligence tools and interagency partnerships to uncover, analyze, and deliver actionable insights. Our capabilities are powered by leading platforms such as Cellebrite, ShadowDragon, and Everbridge 360, and are supported through established data access channels with the Department of Justice, Department of Motor Vehicles, and other government entities. These resources allow us to conduct in-depth investigations with precision, speed, and legal integrity.

Our mission is to seamlessly integrate our protective, investigative, and technological capabilities to empower our clients with quality service and actionable intelligence, enabling them to make informed, risk-aware decisions in complex and dynamic environments. Whether securing a high-profile event, conducting a sensitive investigation, or providing long-term protective services, Peralta Associates and Defense delivers with professionalism, discretion, and results.

PERALTA

ASSOCIATES & DEFENSE

PARTNERSHIPS

WALI

American Red Cross

California Association of Licensed Security Agencies, Guards & Associates

CALSAGA

IALEIA

everbridge

Cellebrite