

What to Expect When You Engage an Executive Protection Provider

A Practical Guide for C-Suite Executives and Security Buyers

Kenneth Wilson, CPO, PPS, EPS | Wilson Global Protection Group

This guide was written for corporate security buyers, C-suite executives, family office principals, and government liaison officers who are evaluating executive protection for the first time — or who have had a previous EP engagement that underdelivered. It covers what a professional EP program actually looks like, how to evaluate providers, what to bring to the first conversation, and where most buyers go wrong.

Executive protection is not a commodity. The difference between a qualified provider and an unqualified one is not always visible until something goes wrong. This guide gives you the framework to make an informed decision before that moment arrives.

CONTENTS

1. Why Most EP Engagements Start Wrong
2. The 5 Phases of a Professional EP Engagement
3. What Separates Qualified Providers from the Rest
4. The Scoping Conversation — What to Bring
5. Red Flags in the Selection Process
6. How Wilson Global Protection Group Works

Section 1: Why Most EP Engagements Start Wrong

The single most common mistake in executive protection is timing. Most clients come to EP after an incident — a threat letter, a confrontation at a public event, a stalking situation that escalated, a kidnapping attempt in a high-risk travel corridor. The reactive posture is understandable. It is also the first mistake.

When you engage EP under duress, you lose negotiating leverage, compress the onboarding timeline, and often accept the first available team rather than the right team. The result is a mismatch between your actual risk profile and the program deployed to address it.

Four patterns account for the majority of poor EP outcomes:

- Clients come to EP after an incident, not before. Reactive posture compresses decision timelines and produces poor provider fit.
- The provider selection process is rushed. When buyers are under pressure, due diligence gets abbreviated. Credentials go unchecked. References go uncalled.
- Corporate buyers don't know what questions to ask. Procurement teams applying vendor-selection frameworks to EP miss the variables that actually matter: advance work capability, intelligence capacity, principal-agent fit.
- The result is mis-calibrated spend. Clients either over-pay for under-qualified teams (large headcount, low tradecraft) or under-buy for genuine risk profiles (one agent for a principal who travels to three developing markets per quarter).

The remedy is straightforward: engage EP before you need it, take the time to evaluate providers against structured criteria, and size the program to the threat rather than to the budget or the optics. The sections that follow give you the framework to do exactly that.

Section 2: The 5 Phases of a Professional EP Engagement

A professionally structured EP engagement is not a single deployment — it is a five-phase program that begins before you are ever visible to the principal and continues after the engagement closes. Understanding these phases lets you evaluate whether a provider is operating at a professional standard or simply providing warm bodies with credentials.

- 1. Threat & Risk Assessment** Before any team is deployed, a credentialed analyst reviews your profile: travel patterns, public exposure, known adversaries, industry threat landscape. This is not optional. A program without a written threat assessment is not EP — it is security theater. The threat assessment determines team size, capability requirements, geographic scope, and advance work priority. Every decision downstream flows from this document.
- 2. Principal Profiling** The detail leader needs to understand your communication style, tolerance for visibility, family dynamics, and schedule patterns. EP that ignores the principal's preferences creates friction and gets fired. The best protective agents in the world are useless if the principal routes around them because the operational tempo is incompatible with the executive's working style. Profiling is not a soft variable — it is an operational requirement.
- 3. Advance Work** Every venue, route, and accommodation is scouted before you arrive. Advance work is where 80% of incidents are prevented. It is invisible when done right. A proper advance includes physical venue assessment, route analysis, hospital and medical facility mapping, emergency egress planning, and coordination with local law enforcement or private security where applicable. If your provider cannot show you an advance report format, they are not doing advance work.
- 4. Close Protection Operations** The visible layer: protective agents, motorcade protocols, venue security coordination. Properly sized to threat level — not to impress. The operational detail executes against the advance plan, maintains principal proximity at appropriate distances, manages access control, and coordinates with venue security and local law enforcement. The detail size should reflect the threat assessment — not the client's desire to project status.
- 5. After-Action & Continuous Improvement** Professional programs conduct post-engagement reviews. Threat environments change; programs should evolve. After-action reporting documents what worked, what was suboptimal, and what threat indicators emerged during the engagement. This feeds the next threat assessment cycle and produces a continuously improving program rather than a static one.

Section 3: What Separates Qualified Providers from the Rest

The executive protection industry is largely unregulated at the federal level. Guard card requirements vary by state, and the credential landscape is fragmented. This creates a wide spectrum of provider quality — from professional close protection firms with intelligence capacity and vetted agents to security guard companies that have added "EP" to their marketing materials without changing their operational model.

Five variables separate qualified providers from the rest:

- **Certifications that matter:** CPO (Certified Protection Officer), PPS (Professional Protection Specialist), and EPS (Executive Protection Specialist) signal tradecraft training, not just a guard card. These credentials require demonstrated competency in threat assessment, advance work, protective driving, and emergency medical response. A guard card means the agent passed a background check and a short state-mandated training program. It does not mean they can run advance work in Lagos or manage a motorcade in midtown Manhattan.
- **Intelligence capability:** Can the provider produce a written threat assessment? Most firms cannot. Intelligence-led EP requires open-source intelligence capacity, a structured analytical methodology, and the ability to translate threat data into operational recommendations. Ask to see a redacted sample threat assessment. If they can't produce one, they are not running an intelligence-led program.
- **Advance work protocol:** Ask to see a sample advance report. If they can't produce one, they don't do real advance work. A credible advance report includes venue floor plans, route maps, hospital mapping, emergency egress routes, local law enforcement contact points, and a site-specific threat assessment. This is operationally intensive work — firms that skip it are cutting the most critical cost center.
- **Discretion record:** Check references. Ask specifically about discretion under pressure. Executive protection agents are in proximity to some of the most sensitive business conversations in corporate America. A single discretion failure — social media post, vendor gossip, information shared with a spouse — can destroy a client relationship and create material legal exposure. Ask references to speak specifically to this.
- **Training lineage:** Where did the principal agents train? Military, federal law enforcement, or dedicated EP programs — not unarmed security guard services. The best EP agents typically come from special operations backgrounds, federal protective details (Secret Service, DSS, USSS), or dedicated EP academies with verifiable curriculum. Ask for agent bios, not just agency credentials.

Section 4: The Scoping Conversation — What to Bring

The first substantive conversation with an EP provider should be a structured scoping session, not a sales call. A professional provider will use this time to understand your threat environment, principal profile, operational requirements, and budget parameters — and will come prepared with questions. Your job is to come prepared with answers.

Bring the following to a first scoping conversation:

- Travel calendar for the next 90 days (domestic + international). Include all confirmed travel — board meetings, investor conferences, site visits, personal travel to high-risk destinations. The provider needs to assess geographic threat environments, advance work requirements, and team deployment logistics. An incomplete calendar produces an incomplete program.
- Any known threat indicators. This includes active litigation with a hostile party, activist campaigns targeting your organization, public disputes with high-profile individuals, prior incidents (threats, confrontations, stalking behavior), and any recent changes in your public profile that may have increased exposure (IPO, major acquisition, high-profile media coverage).
- Principal profile. Who requires coverage? The executive principal, immediate family members, board members traveling with the principal? Are there known public exposure points — recurring public appearances, predictable routines, high-visibility philanthropic commitments? The provider needs this to size the detail and scope the advance work correctly.
- Budget range and internal security team structure. If you have an existing corporate security function, the EP detail needs to integrate with it — not replace it. If you don't, the provider needs to understand whether they are building a standalone program or augmenting informal security arrangements. Budget clarity avoids the most common friction point in EP engagements.
- Decision timeline and key stakeholders. Who is involved in the selection decision? General counsel, CISO, CFO, board security committee? What is the required start date? Is there a contract vehicle the provider must be registered to? The more you can share about the procurement process, the faster a professional provider can move to program design.

A scoping conversation is not a commitment. It is the mechanism by which a professional provider determines what program you actually need — and whether they are the right fit to deliver it. Be as transparent as possible. The more context the provider has, the more accurate the program recommendation will be.

Section 5: Red Flags in the Selection Process

The EP sales process is designed to instill confidence. Most providers will present credentials, reference high-profile past clients (without disclosing them by name), and describe operational capabilities in language that sounds authoritative. The red flags that separate credible programs from underqualified ones are not always visible in the presentation — they emerge when you ask the right questions.

Six red flags warrant immediate caution:

- No written threat assessment methodology. If a provider cannot describe their threat assessment process in specific terms — what data sources they use, what analytical framework they apply, what format the output takes — they are not running intelligence-led EP. This is the foundation of the entire program. Absence here is disqualifying.
- Inability to provide verifiable references from comparable clients. Every professional EP firm has a client confidentiality obligation, and references will be redacted accordingly. But a credible provider can connect you with references who can speak to the operational quality of the program without disclosing protected principal information. If a provider cannot produce any verifiable references, proceed with caution.
- Aggressive upselling on team size without threat justification. A provider who recommends a six-person detail before completing a threat assessment is selling headcount, not security. Team size is a function of threat level, principal profile, and operational environment — not of what generates the highest retainer. Any team size recommendation should come with a written threat justification.
- No advance work capability. If the provider does not have a documented advance work protocol — and cannot show you what an advance report looks like — they are not running professional EP operations. This is not a secondary capability. Advance work is where the majority of incidents are prevented. A provider without it is leaving the most critical protective function unaddressed.
- Pricing that seems too low. Executive protection is labor-intensive. A credentialed, trained protective agent in a major market commands significant compensation. Low prices in EP mean one of three things: underqualified staff, dangerously low agent-to-principal ratios, or hidden costs that appear in the first invoice. Evaluate pricing in the context of what is actually included, not against a market average.
- Resistance to background checks on their own agents. Every agent in proximity to your principal should be subject to a background check, and a professional provider will facilitate this without objection. Resistance — whether framed as a legal concern, a confidentiality issue, or an operational necessity — is a red flag. You have the right to know who is in your detail.

Section 6: How Wilson Global Protection Group Works

Wilson Global Protection Group is a professional executive protection firm led by Kenneth Wilson, CPO, PPS, EPS. We serve C-suite executives, government dignitaries, family offices, and corporate security programs across North America and internationally. Our operating model is built around the intelligence-led, advance-first framework described in this guide.

Our engagement model is structured as follows:

- Every engagement begins with a 60-minute scoping consultation (\$500, credited toward your engagement). The scoping session is structured: we review your threat indicators, travel calendar, principal profile, and existing security posture. The output is a written program recommendation with cost parameters.
- We produce a written threat assessment before any deployment recommendation. No program is designed without one. The threat assessment is the analytical foundation of everything that follows — team sizing, advance work scope, operational protocols, and geographic prioritization.
- Our principals hold CPO, PPS, and EPS credentials — not guard card certifications. Our agents are drawn from special operations, federal law enforcement, and dedicated EP training programs. We do not deploy unarmed security personnel in protective roles.
- We operate with full discretion: no social media, no visible branding on vehicles or personnel, no disclosure of client identity without explicit authorization. Our agents sign comprehensive non-disclosure agreements as a condition of engagement. Discretion is not a policy — it is an operational discipline.
- We serve clients across North America and internationally, with particular capability in high-risk travel corridors in Latin America, Africa, and the Middle East. Our international programs include in-country advance work, local law enforcement liaison, and emergency extraction planning where threat profiles warrant it.

Ready to Start the Conversation?

Book your 60-minute scoping consultation. The \$500 fee is credited toward your engagement.

grandiose-goshawk-617.convex.site/checkout/wilson-global-protection-group/md70wbw4qrjsgy6rbded0xm7f185ya5w

Contact: team@wilson-global-protection-group.madethis.app

About the Author

Kenneth Wilson is a Certified Protection Officer (CPO), Professional Protection Specialist (PPS), and Executive Protection Specialist (EPS) with extensive experience protecting C-suite executives, government dignitaries, and high-net-worth principals across domestic and international environments. He is the founder and principal of Wilson Global Protection Group.

Wilson Global Protection Group provides close protection, threat assessment, security consulting, crisis management, and travel security services to corporate clients, family offices, and government agencies across North America and internationally.

Key Takeaways

- Engage EP proactively — before an incident forces a reactive and rushed decision.
- Require a written threat assessment before accepting any program recommendation.
- Evaluate advance work capability as a primary differentiator — it is where most incidents are prevented.
- Ask for verifiable references and check them specifically for discretion under pressure.
- Size team to threat, not to appearance. A proper threat assessment drives this recommendation.
- Background check every agent in your detail. A professional provider will facilitate this without objection.
- Bring a complete travel calendar, threat indicators, and principal profile to the scoping conversation.
- Treat pricing-that-seems-too-low as a red flag, not a value proposition.

This guide is provided for informational purposes. It does not constitute legal, security, or operational advice for any specific situation. For a program recommendation tailored to your threat environment and principal profile, contact Wilson Global Protection Group to schedule a scoping consultation.

WILSON GLOBAL PROTECTION GROUP

team@wilson-global-protection-group.madethis.app

© 2026 Wilson Global Protection Group. All rights reserved.