THE HAGUE
10 Oct. 2024

7th European Security Summit

CoESS | Nederlandse Veiligheidsbranche | International SecurityLigue

WHITE PAPER

Public-Private Partnerships: Unlocking the Potential for Enhanced Security

About the Authors of the Paper:

The **Confederation of European Security Services (CoESS)** has represented the private security industry across Europe for 35 years. CoESS is dedicated to promoting high standards of professionalism and quality within the security industry, advocating for policies that support the sector's growth and professionalism.

The **Nederlandse Veiligheidsbranche** (the Dutch Security Association) has been the representative of the Dutch security industry for 85 years. The organisation defends the interest of the companies in the security sector on a national level, maintaining contacts with government, parliament and other stakeholders. The Nederlandse Veiligheidsbranche unites SMEs and large certified companies, represents 90% of market turnover and its' members employ 32.000 qualified security guards.

The **International Security Ligue** is the global association of private security organizations, dedicated to advancing security standards worldwide. With a focus on promoting best practices and fostering international cooperation, the International Security Ligue provides a global perspective on security challenges and solutions. Their contributions help to contextualize the discussion within a broader international framework.

Design & graphics:

https://blog.acapella.be/

Photo credits:

© AdobeStock: 189459003: Patrick Daxenbichler, 734099125*: PikePicture, 490783520: Pixel-Shot, 920222022*: Andres Mejia, 856511461*: Curioposs, 546319561: NongAsimo

Generated with AI

© iStock: 1461413822: HJBC, 1316755706: Flex Point Security, 836601774 and 836601946: Naypong, 1219733094: MARHARYTA MARKO, 1575562418: Jacob Wackerhausen, 1393855287: Galeanu Mihai, 1281959537: NicoElNino, 1472468738: Irene Puzankova, 1498077737: CASEZY, 1444503376: Marta fernandez, 1480307525: gorodenkoff, 1460172015: Tippapatt, 506815322: artJazz, 908827618: AndreyPopov

© Shutterstock: 131124554: Michael Dechev

Acknowledgements:

CoESS is deeply grateful to the following people for their detailed review, sharing their knowledge and expertise and providing improvements to this document:
Eduardo Cobas Urcelay, Secretary General, APROSER
Alexander Frank, Deputy Director General, CoESS
Jonas Maas, PhD Researcher, Department of Criminology, Criminal Law and Social Law, IRCP, Ghent University
Drs. René R.K. Siccama Hiemstra, Director, G4S Netherlands
Garett Seivold, Chief Content & Communications Officer, The International Security Ligue

Disclaimer:

Our liability—to the fullest extent possible at law we (and all our sister, parent, subsidiary and member companies and organisations) exclude all liability for any loss or damage (including direct, indirect, economic, or consequential loss or damage) suffered by you because of using the contents of this document.

Publisher:

Catherine Piana
Director General
CoESS aisbl
56 Avenue des Arts
1000 Brussels
Belgium
catherine@coess.eu
www.coess.eu

TABLE OF CONTENTS

Foreword 4

Executive Summary 5

1. Introduction 8

2. PPPs: definitions, scope and relevance 10

3. Opportunities, Success Criteria and Challenges in PPPs 14

4. Mapping out of PPPs in Europe 20

5. Policy and Strategic Recommendations 22

6. Best Practice 24

7. The International Security Ligue's Checklist for Building an Effective Private Security Partnership 34

Foreword

The private security industry is increasingly recognized as a vital partner to Law Enforcement Agencies (LEAs) in ensuring the protection of people, assets, and infrastructure. This recognition has accelerated in recent years, driven by significant global challenges such as the COVID-19 pandemic and the persistent threat of terrorism. Throughout these crises, Private Security Companies (PSCs) and their dedicated staff have demonstrated their unwavering commitment to safeguarding society, taking on critical roles in prevention and protection.

As a result, governments across Europe are turning more frequently to the private security industry for support, especially in light of the labour shortages affecting LEAs. While law enforcement must remain focused on their core missions, PSCs are well-positioned to perform a range of complementary tasks. This partnership has proven not only efficient but necessary, as PSCs bring professionalism, innovation, and cutting-edge technology to the table – essential elements in modern security strategies.

Although privately owned and commercially driven, PSCs can be a great contribution to safety in the public domain, both as a contracted supplier or as a contributor using the eyes and ears of the 2 million guards in Europe who give their best on a daily basis to make our world a safer place.

Public-Private Partnerships (PPPs) present a tremendous opportunity to enhance security outcomes through complementarity. The success of these partnerships is made possible by the increasing professionalism of the private security industry and its ability to innovate. With the right legal frameworks, PSCs can support LEAs in a wide range of missions, freeing up public resources for more specialized law enforcement tasks.

We call on authorities to continue fostering these partnerships, seeing PSCs not as subordinates, but as essential partners in the security continuum. At the same time, we urge the private security industry to embrace this evolving role, continuing to demonstrate leadership and commitment to the protection of our societies. Together, we can build a stronger, more resilient security framework that is better equipped to meet the challenges of today and tomorrow.

Vinz van Es,
Chairman,
CoESS

Ard van der Steur,
Chairman, Nederlandse Veiligheidsbranche (NVB)

Executive Summary

This White Paper aims to identify, define, and describe Public-Private Partnerships (PPPs) in Europe, highlighting their crucial role in enhancing security across various environments. By drawing on theoretical sources and showcasing best practices, it demonstrates how collaboration between Law Enforcement Agencies (LEAs) and Private Security Companies (PSCs) strengthens overall security and societal resilience. Additionally, the paper addresses the challenges that hinder the effectiveness of PPPs and offers recommendations for stakeholders to overcome these barriers, implement key success criteria, and optimize the potential of PPPs.

An Opportunity for Complementarity and Increased Efficiency

Public-Private Partnerships considered in this paper are all forms of cooperation between LEAs and PSCs. As such, they combine the strengths and resources of public security forces with the specialized capabilities of private security companies. This collaboration addresses complex security challenges efficiently, ensuring a comprehensive approach to the protection of people, assets and infrastructure, and thus society as a whole. The synergy allows for an extended security reach, leverages advanced technologies, and enhances the strategic allocation of resources across the security spectrum.

Significance and Impact

PPPs are shown to optimize the use of resources, allowing LEAs to focus on their core tasks while PSCs address the prevention and detection dimensions. The partnerships enhance operational capabilities, provide scalability in response to changing security demands, and introduce innovative solutions to security management. This strategic collaboration leads to improved flexibility in operations and a proactive stance in security planning.

Highlights

PPPs are legally possible in only 9 out of 27 EU Member States and mostly in Western European countries, where they cover different realities. While some Member States have advanced partnerships based on formal frameworks, others are informal, local and temporary. The type of protected objects and events also vary, as do the missions that are given to the PSCs.

There is a correlation between the level of professionalism of the industry, the maturity of the legal framework, and the depth of cooperation between LEAs and PSCs.

This paper describes the advantages in operating PPPs, including:

- Resource Efficiency: Private companies support LEAs by handling preventive and surveillance tasks, freeing up public resources for LEAs to concentrate on their core missions.
- Advanced Specialization: PPPs bring state-of-the-art technology and specialized skills, particularly valuable in areas in which they have developed particular know-how, such as access control, distance surveillance and monitoring, protecting certain infrastructure (critical and others), etc.
- Strategic Flexibility: The ability to dynamically scale security measures in response to situational analyses enhances both proactive and reactive capabilities.

Implications for the Security Landscape

The increased complexity and diversity of threats require a shift towards a more integrated and responsive security framework. This approach not only improves immediate responses to threats but also supports a sustained security strategy that adapts to future challenges. The implications extend beyond immediate security enhancements, suggesting long-term benefits in public safety and trust.

Challenges and Strategies for Overcoming Obstacles in PPPs

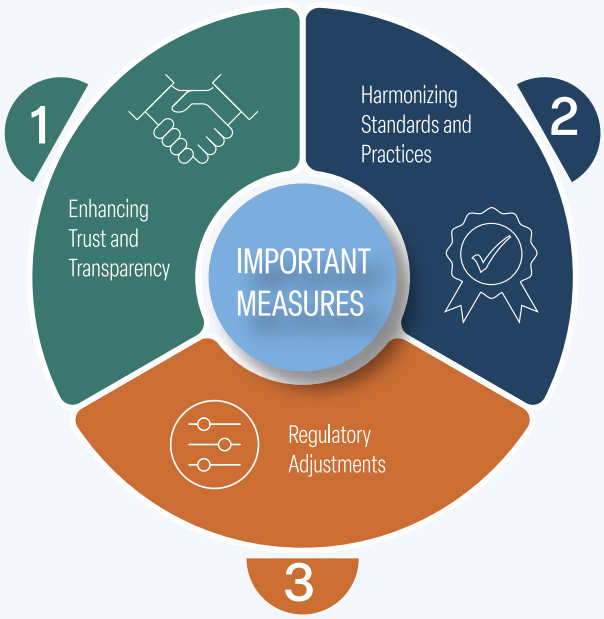
While Public-Private Partnerships offer substantial benefits, they also face specific challenges that can hinder their effectiveness. Key obstacles include issues of trust and information sharing, differing operational cultures between public and private entities, and regulatory constraints that can stifle collaborative efforts.

To overcome these challenges, this White Paper recommends several measures, of which the following are particularly important:

1. Enhancing Trust and Transparency: Building trust is fundamental. Initiatives such as joint training sessions, shared operational planning, and regular stakeholder meetings can foster a mutual understanding and strengthen trust. Clear communication and transparency in operations and decision-making processes are crucial for developing a reliable partnership.

2. Harmonizing Standards and Practices: Developing common standards and practices across public and private sectors within PPPs can alleviate cultural and operational discrepancies. Areas to look into may include training, security protocols, data interoperability, vulnerability assessments and complementarity in response strategies to optimise cooperation.

3. Regulatory Adjustments: Modifying existing laws and regulations to support PPP frameworks and allow for the exchange of information between PSCs and LEAs is essential. Legislation should support best value procurement, collaborative actions and facilitate rather than inhibit information sharing, ensuring that both public and private entities operate under a supportive legal framework that will help reinforce mutual trust and promote cooperation. Finally, legislation should also provide that LEAs have a good understanding of what PSCs can and can't do. This could be included in basic LEA staff training.



"PPPs not only enhance current security measures but also prepare organizations for emerging threats."

By addressing these challenges through targeted strategies, PPPs can not only enhance their operational effectiveness but also achieve a more resilient and adaptive security infrastructure. These efforts require ongoing commitment and adaptation from all stakeholders involved to ensure the continued success and evolution of PPPs in the security sector.

In conclusion, Public-Private Partnerships are indispensable in the modern security apparatus. By effectively combining the unique strengths of LEAs and PSCs, PPPs not only enhance current security measures but also prepare organizations for emerging threats. This White Paper supports the continued development and refinement of PPP frameworks to maximize their positive impact on public security.

1. Introduction

This White Paper on Public-Private Partnerships (PPPs) in Security is a collaborative effort by the European, Dutch and International organizations in the security industry: the Confederation of European Security Services (CoESS), the Nederlandse Veiligheidsbranche (NVB), with the support of the International Security Ligue (ISL). These organizations bring a wealth of expertise and experience to the table, providing a comprehensive and authoritative perspective on the evolving landscape of private security, including how it cooperates with Law Enforcement Agencies (LEAs) in the protection of people, assets and infrastructure.

Building upon the foundation laid by the CoESS White Paper on the Security Continuum in the New Normal[1] this document delves deeper into the dynamics of public-private partnerships in the security sector. The publication highlighted the need for seamless cooperation between public and private security entities to address contemporary security challenges effectively. This White Paper aims to expand on that concept, offering new insights, strategies, and recommendations for enhancing public-private collaboration in the security sector. In particular, the paper will map out the status of PPPs across Europe, outline the opportunity for authorities, list the obstacles and solutions, and make recommendations for the future.

[1] *Confederation of European Security Services (CoESS). (2019). "The Security Continuum in the New Normal". Retrieved from https://coess.eu/.*

Objectives of the Paper:

1. Define PPPs in Security in Europe: **Chapter 2** aims to clarify the concept of PPPs within the European security context, establishing a clear definition and scope that encompasses the various forms and structures of collaboration between PSCs and LEAs in different countries and within their respective legal frameworks.

2. Outline the Opportunities and the Success Criteria of PPPs: the first part of **Chapter 3** explores key factors contributing to the success of PPPs in the security sector, such as trust, effective communication, a supportive legal framework and interoperable technology. It will examine how these elements foster a productive partnership that enhances overall security outcomes.

3. Identify and Analyze Obstacles: Despite the potential benefits, several challenges hinder the effectiveness of PPPs. The second part of Chapter 3 will discuss common obstacles such as building trust between entities with different cultures and operational philosophies, creating mutual understanding of complementary roles, and establishing a shared mindset of active collaboration. It includes a dedicated section on the sensitive issue of the exchange of information.

4. Present Existing Models: By showcasing various successful PPP models, **Chapter 4** and **6** will provide concrete examples of how these collaborations work in practice. These case studies will highlight the operational details, governance structures, and the specific contexts in which these partnerships flourish.

5. Recommendations to the various PPP Stakeholders: **Chapter 5** draws from best practice and academic literature on PPPs to propose innovative approaches and solutions. This discussion aims to inspire readers and provide them with actionable strategies to enhance the implementation and effectiveness of PPPs in their own contexts.

Finally, in **Chapter 7**, we include a checklist drawn up by the International Security Ligue on "Building an Effective Private Security Partnership". It categorizes and lists criteria considered by the Industry as relevant to evaluate the capacity of a PSC to enter into a partnership.

Through these objectives, this White Paper intends to continue and deepen the conversation to explore how we can better work together and forge stronger, more effective partnerships that can meet the complex security challenges of today's world. By providing a thorough understanding of both the mechanisms and the challenges of PPPs, the paper seeks to pave the way for more integrated and effective security strategies across Europe and beyond.

"This White Paper explores how we can better work together and forge stronger, more effective partnerships."

2. PPPs: definitions, scope and relevance

"Tasks and competencies of PSCs, and with it concepts of PPPs, differ among European countries."

2.1. Definition and scope of PPPs in the context of security and this paper

While there are several definitions of PPPs, this paper takes a wide and flexible perspective, whereby it looks at all the situations where the police or other Law Enforcement Agencies (LEAs) work with the private security industry, namely:

- A Private Security Company (PSC) protects a publicly accessible or other location on behalf of and/or under the supervision of Law Enforcement;
- The tasks performed by a PSC requires some form of collaboration between this company and an LEA. This includes the protection and access control of places that are privately owned and are accessible to the general public, such as shopping areas, cultural landmarks, and places of worship, as well as Critical Infrastructure or other sensitive sites and events. The cooperation with LEAs is needed in preventive measures, by understanding the potential risks and threats, and if LEA intervention is needed. Law enforcement and public security are a national competence. Hence, tasks and competencies of PSCs, and with it concepts of PPPs, differ among Europe countries. We are therefore looking at many different models of PPPs, which in turn are influenced by the respective national legislation.

2.2. The economic, social and operational rationale for PPPs and how they enhance security outcomes

Europe is made of a myriad of different models, legal frameworks and approaches to having private companies perform tasks on behalf of the LEAs

or in cooperation with them. Also, these differing legal systems have a different boundary between missions performed by the LEAs and by private security. While there is a hard line around the core LEA missions and tasks, there is a softer one around those more peripheral tasks that do not involve authority or (monopoly of) force and fluctuates from country to country. This is the area where more tasks may benefit from the support of private security. However, for this to happen, governments, LEAs and society need to acknowledge, accept and trust this PPP construct. In her paper[2] , L.A Bisschops, a Criminologist who wrote her Master's thesis about PPPs in 2022, highlights the fact that that multiple elements related to strengthening public-private partnerships are depending on the political climate.

Where PPPs exist, they are mostly the result of various factors and drivers:

- Ongoing capacity challenges in LEAs due among others to labour shortages, and ability of Private Security Companies to compensate for them, thereby enhancing cost efficiency;
- Insufficient public resources to perform all security and prevention issues;
- Rising crime rates and/or the demand for more security, which can't all be met by LEAs;
- The increasing complexity and scope of security challenges, requiring the involvement of specialised staff, which is not necessarily available in LEAs;
- Professionalisation and digitalization of the security sector, whereby PSCs have invested in training, technology and infrastructure to enhance their capabilities;

Until now, public-private partnerships have been an attractive way to optimize risk distribution, under the assumption that private parties applied risk allocation more efficiently than public organizations, while public parties were better able to address all administrative aspects more effectively. However, circumstances now suggest that public-private partnerships are not so much attractive as they are necessary. The performance of organizations in the security sector, both public and private, is under pressure in the rapidly changing threat landscape against the backdrop of a structurally problematic labour market.

Because of the nature of services provided by it, the private security industry is able to provide support to the LEAs by taking over missions that are not part of their core tasks and bring its expertise as a complement to specific LEAs' missions and prerogatives.

2.3. Overview of PPP concepts and models

Types of PPPs are numerous and, in this document, we include examples such as:

- Sharing information: private security report to the LEAs about suspicious behaviours or persons and vice-versa;
- Prevention of illegal actions: access control in spaces accessible to the public, such as sports or cultural events or locations, transport hubs, etc.
- Collaboration in exercises and trainings;
- Risk assessments and vulnerability assessments;
- Protection of Critical Infrastructure: while this will be the focus of a future CoESS paper, there are a couple of examples used in this paper showing how PPPs can enhance the protection and resilience of CI. In the current context of the war in Ukraine, PSCs are increasingly called upon not only to protect military infrastructure with different human and technological means but to consider additional means to support countries in case they need to become actively involved in the conflict.

[2] *Bisschops, L. A. (2022). Een internationaal kwalitatief onderzoek naar het verstevigen van publiek-private samenwerking in het Nederlandse veiligheidsdomein – translation: An international qualitative study on strengthening public-private partnerships in the Dutch security domain [Master's thesis, University of Amsterdam, Investigative Criminology].*

KEY COMPONENTS OF SUCCESSFUL PPPs RECOMMENDATIONS FROM THE CoESS WHITE PAPER ON THE SECURITY CONTINUUM IN THE NEW NORMAL

In the White Paper on the "Security Continuum in the New Normal", CoESS articulated the success criteria for PPPs around 4 core values:

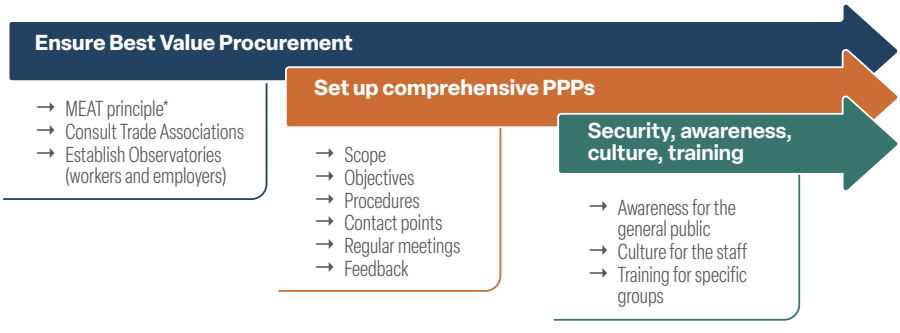
Safety: ensuring the protection and safety of the client's and the provider's staff by selecting only legitimate companies to enter into PPPs. PSCs need to demonstrate that security officers are duly licensed, selected and trained and that working conditions ensure that they are well equipped and protected.

Compliance: making sure that companies strictly comply with the laws and regulations, and the industry standards and certifications.

Quality: because security is a specific type of service, the element of cost should never be the only criteria taken into account when establishing a PPP. The EU Social Partners in Private Security Services, CoESS and UNI Europa, have jointly published a manual for "Buying quality private security services[3]", which explains how to measure quality objectively and select best value providers, as opposed to the cheapest ones.

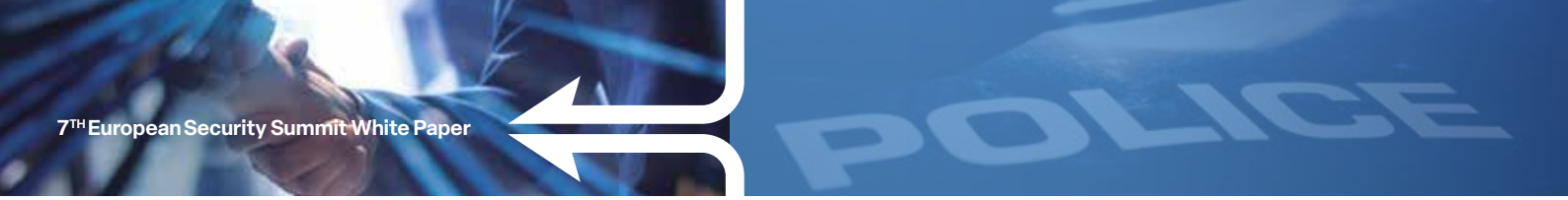
Trust and public acceptance: it is quite obvious that there can be no partnership without trust between those involved and, more widely, from citizens whose protection is ultimately at stake in these partnerships.

In the paper, CoESS regretted that there were no general frameworks for PPPs, nor were there protocols for the exchange of information. The paper suggested 3 successive steps to be set up in order to conclude PPPs, which can be summarised in the following graph:



**Note: MEAT stands for Most Economically Advantageous Tender. It is a method of assessment that can be used as the selection procedure, allowing the contracting party to award the contract based on aspects of the tender submission other than just price.*

[3] *CoESS and UNI Europa. (2014). Buying Quality Private Security Services. https://www.securebestvalue.org/.*



THE EUROPEAN COMMISSION'S "GOOD PRACTICES TO SUPPORT THE PROTECTION OF PUBLIC SPACES" AND RECOMMENDATIONS FOR PUBLIC-PRIVATE COLLABORATION

An important baseline for public-private collaboration in the protection of public spaces is the European Commission Staff Working Document 2019/140[4] on "Good practices to support the protection of public spaces", which was developed jointly by the Commission, Member State authorities, operators of public spaces, and the Confederation of European Security Services (CoESS). Regarding public-private collaboration, important good practices include:

- **Security Culture:** Development of a common culture of security, shared between public authorities, private actors, and citizens.

- **Vulnerability and Risk Assessments:**
  - Regular vulnerability assessments to be conducted in a public-private collaboration approach, followed by tailor-made security measures.
  - Public authorities should share risk assessments and information as appropriate, and a trustful and timely communication and cooperation that allows for a specific risk and threat information exchange between responsible public authorities, local law enforcement and the private sector should be established.

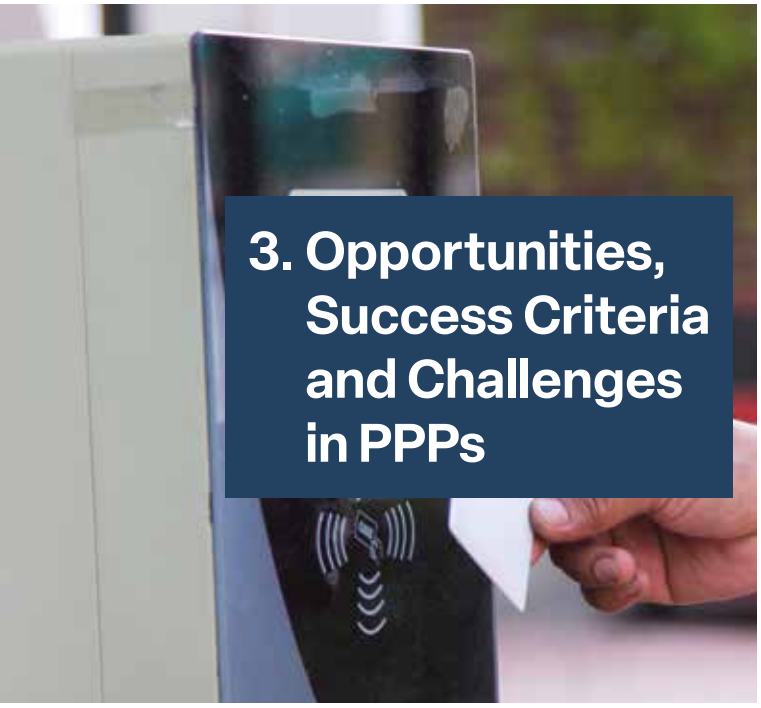
- **Clear Roles, Responsibilities and Communication:**
  - Public and private operators should appoint a competent person, as well as a backup, who understands the threats landscape and knows well the facility/event and make sure that this person receives the appropriate training.
  - Every actor involved in the security chain should appoint contact points and clarify respective roles and responsibilities in public-private cooperation on security matters (e.g. between operators, private security and law enforcement authorities) and for a better communication and cooperation on a regular basis.
  - Operators shall ensure efficient management and communication in crisis situations with staff and customers, as well as with law enforcement, with the help of technology, crisis communications teams and clear messaging.

- **Training:**
  - Staff working at the facility or event should be properly trained and regularly re-trained for the tools they operate.
  - Undertake regular security exercises that will help to identify the level of preparedness to deter and respond to an attack, involving all relevant stakeholders (e.g. rescue services, special forces and other relevant service providers).

- **Physical Protection:** Public and private entities need to be involved to better take into account protection issues in the design of buildings and other spaces.

- **Insider Threats:** Based on the vulnerability assessment, and in close cooperation with law enforcement authorities, operators of public spaces should consider background checks and possible vetting of the staff in respect of national laws both before and during their assignments. The EU-funded AITRAP project (www.help2protect.info) which was coordinated by CoESS, provides an Insider Threat online training programme and is a good example for such a tool.

[4] *European Commission. (2019). Commission Staff Working Document: Assessment of the 2018 Country Reports on the implementation of the European Union's legal framework on data protection.*



3. Opportunities, Success Criteria and Challenges in PPPs

"Private security complements law enforcement by offering unique skills and perspectives that enhance overall security efforts."

3.1. Opportunities

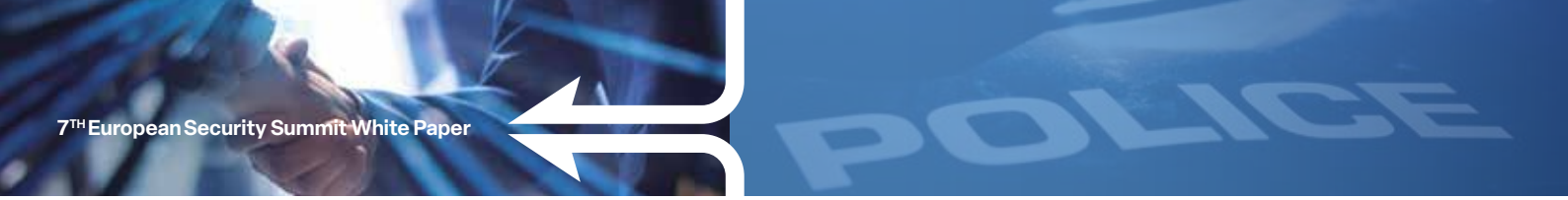
The main opportunity of PPPs is the complementarity that it presents between its players' strengths:

From the public side:

- Authority and the use of force if required
- Intelligence gathered by specialised government agencies
- Access to classified information
- Legitimacy in carrying out these missions and trust from citizens
- Accountability and scrutiny

From the private side:

- **Operational Expertise & Workforce Support:** PSCs provide specialized expertise in prevention and detection, employing advanced technologies like digital surveillance, and risk assessment not always available to LEAs. By taking on these roles under regulated and strictly overseen conditions, PSCs not only alleviate LEA resources, allowing them to focus on specialized tasks such as counterterrorism, but also enhance overall security effectiveness without compromising public security control. This partnership enables LEAs to utilize private sector capabilities more strategically.
- **Enhanced Security & Specialized Knowledge:** Private security complements law enforcement by offering unique skills and perspectives that enhance overall security efforts, particularly in specialized areas like airport security where passenger and baggage screening are efficiently managed by PSCs. With extensive experience in securing critical infrastructure and public spaces, PSCs focus on early prevention and detection within the criminal planning cycle, allowing both parties to concentrate on their core competencies. This contributes significant capacities to security operations and allows



PSCs to respond swiftly to urgent needs, often quicker than LEAs.

- **Innovative Technologies and Resources to Operate them:** Companies invest in training personnel and applying state-of-the-art technologies to offer the best security solutions, continuously assessing risks to enhance resilience in an evolving threat landscape. Unlike LEAs, which lack competitive pressure and client-driven responsiveness, PSCs are more attuned to market needs. Additionally, technology facilitates better coordination and cooperation with public forces, such as sharing video surveillance with LEAs. In line with the "New Security Company[5]" concept, PSCs increasingly adopt an integrated security approach that combines people, technology, and processes, including investments in the connected officer.

- **A Culture of Efficiency and Measuring Performance:** PSCs operate in a competitive environment that promotes a strong culture of performance measurement. This culture benefits LEAs by introducing rigorous standards and metrics to assess security protocols. PSCs use these metrics to evaluate the effectiveness of their security measures, providing a model that LEAs can use to improve their operations. Adopting these practices helps enhance LEA performance, align security measures with measurable outcomes, and potentially increase public trust and satisfaction. By combining these strengths, risks can be better mitigated, and the resilience of the protected objects, reinforced.

3.2. Success Criteria

For the PPP to optimise the complementarity, several elements need to be present.

By taking up the criteria in the White Paper on The Security Continuum in the New Nlormal, the European Commission Recommendation, the observations made in the SAFE-CITIES project, reviewing literature about PPPs, and interviewing PPP stakeholders, we consider that the following criteria are needed for success:

I. Trust

a. Trust among Partners: This includes trust between leaders from each side and nurturing a trust culture among those involved in executing the PPP, ensuring all participants believe in the reliability and integrity of their counterparts.

b. Trust in Processes: Ensuring clear roles and responsibilities, transparency in how resources are used, and explicit, accountable decision-making processes.

c. Trust in Technology: Emphasizing the security, interoperability, and protection of data used in support of the PPP, including safe and cybersecure channels for live data exchange.

d. Selection of Quality Service Providers: Choosing partners that uphold high standards of quality and professionalism contributes significantly to the trust and efficacy of the partnership.

II. Competency and Value Acknowledgement

a. Recognizing and valuing the unique competencies each partner brings to the table, understanding how these competencies contribute value to the partnership's overall goals.

III. Communication and Collaboration

a. Facilitating open communication and the timely exchange of relevant information to ensure all partners are informed and engaged. This includes sharing a common taxonomy and vocabulary between LEAs and PSCs.

b. Promoting a collaborative mindset where all parties acknowledge their shared interests in achieving common goals.

c. Aligning training programmes in all areas required.

[5] *This concept is described in the CoESS-BDSW White Paper on "The Security Company: integration of services and technology responding to changes in customer demand, demography and technology" - 2015.*

IV. Culture and Flexibility

a. Fostering a culture of honesty and justice, where giving feedback is encouraged in a spirit of continuous improvement, and mistakes are treated as learning opportunities, and not causes for punitive measures.

b. Maintaining flexibility within the partnership, allowing for continuous assessment and evolution to adapt to new challenges and opportunities.

c. Ensuring that the culture permeates all layers of the hierarchy of both the LEAs and PSCs, top-down and bottom-up.

V. Legal Framework and Government Connection

a. Establishing a robust legal framework that clearly defines roles, responsibilities, and operational boundaries for private security companies within the industry and making sure they are communicated to and understood by all those involved.

b. Ensuring the framework supports regular evaluations of the partnership to align with public safety and security goals.

c. Enhancing the connection between government and private security networks to ensure transparency, accountability, and regular updates on performance and strategic alignment.

d. Facilitating a framework that pools resources in terms of personnel and technologies, thereby enhancing operational capabilities and efficiency.

VI. Data and Technology Management

a. Prioritizing data interoperability to allow seamless communication and information sharing across diverse platforms and organizations.

b. Implementing frameworks for information exchange that are clear, structured, and capable of supporting complex operational requirements without compromising security.

3.3. Main areas for improvement

Based on literature and interviews with PPP stakeholders, the following areas are those where progress is most needed. Avenues for solutions are discussed in section 5.

- The lack of formal and comprehensive frameworks and appropriate legislation for the PPPs:
  - PPPs are very often based on good will and personal relations. If one of the main players of the PPP moves on to another job or retirement, the PPP may suffer or cease to exist.
  - There is often no general framework to which the partners can refer, and thus they rely on interpretation or expectations.
  - Legislation often does not include provisions to establish partnerships or allow and regulate the exchange of information between LEAs and PSCs.

- Mutual recognition of competencies and skills: there is a lack of understanding and knowledge among Law Enforcement of private security officers' skills and competencies, which may affect the cooperation and personal relations within the partnership. Several experts suggested that in their basic training, LEA staff should receive detailed information about the legal framework within which PSCs and private security officers operate, including their missions and limitations.

- Effective communication between LEAs and PSCs includes using the same taxonomy and vocabulary to communicate. In an interview with a PSC and their LEA counterpart, they highlighted that the use by PSC staff of the LEA's specific information "coding" was a game changer in the LEA's consideration of PSC reports. The LEA gave credibility to the reports because they were passed on in their language and PSC interlocutors felt they were taken seriously and were better considered.

- Address the issue of cost: in their paper on PPPs[6], Steden and Meijer recommend that private parties can be involved more closely in the PPP if they are enabled to charge costs to their clients or if the costs are divided more fairly among the participating parties. In the best practices explored in Chapter 6, in most cases costs are either not mentioned or are explicitely mentioned as being fully borne by the PSC.

- Creating a true partnership bearing in mind the disparity between public and private stakeholders.

[6] *Steden, R. van, & Meijer, R. (2018). Publiek-private samenwerking in tijden van diffuse dreiging: Een onderzoek naar diversiteit in werkwijzen en kansen in de Nederlandse en Vlaamse context. Den Haag: WODC.*

A particularly sensitive issue: the exchange of information

In a sensitive area such as the exchange of information, for which there is by nature a strong reluctance in security communities, even between LEAs, there is a need to explain why this is useful and necessary and how everyone will ultimately benefit. How the exchange of information can be done while remaining in compliance with GDPR is also a matter for deeper analysis. The following section seeks to highlight the advantages of creating such exchange. It is also important to stress the fact that the information collected by the LEAs is not necessarily useful as such. What private actors may be interested in is the "actionable" part of the information or intelligence. Case in point: it may not be useful for the private players to identify the authors of an unlawful action, but rather how an unlawful act might affect them. For example, the fact that there has been a terrorist attack at a certain location is useful information for PSCs protecting locations or objects within a certain radius of the initially attacked object. This is not a breach of an ongoing investigation and only a matter of time before the information becomes public.

It might be useful to carry out a survey among PSCs and the LEAs about the kind of information and intel, which could be useful and in what format it could be passed on.

The advantages of better information exchange:

- Crime Scripting: Better threat assessments by identifying trends and patterns
- Predictive Policing: Enhanced ability to predict security incidents and criminal offences
- Improved operational efficiencies and resource allocation, and better targeting of patrols
- Enhanced staff preparation and thus enhanced staff safety
- Ability to better see the broader picture
- Creating continuity between the various players, and thus reducing vulnerabilities
- Overall better decision-making and better service delivery
- Providing learning opportunities for all players in the partnership

The challenges in sharing information:

- Different mandates and legal capacities
- Data protection and privacy law and security, and its interpretation, incl. interoperability
- Lack of trust

Avenues for solutions:

- Creating and documenting procedures for the exchange of information to provide clarity and transparency. This is further explained in the ISO 22396:2020 Standard, "Guidelines for information exchange between organisations".
  - By using existing tools for the exchange of information:
    - Security clearances at various levels
    - Non-disclosure agreements (NDAs) in accordance with the Traffic Light Protocol (TLP)[7]

- Clarifying national interpretation of GDPR and other legislation concerning data protection to help ease concerns about privacy by removing some of the uncertainty that they carry. CoESS has signed a letter of 23 sectors to the Commission, calling for a reaffirmation of the Regulation's risk-based approach as its guiding principle[8].

- Reinforcing trust:
  - By encouraging in-person contacts and regular meetings
  - By creating hybrid (public and private) teams, and/or creating liaison posts in each of them, where trusted individuals (information "brokers") are designated for the exchange of information.
  - By providing feedback on the uses of information provided by the contributor, and enhance the feeling of contribution.

- Showing commitment to security culture and data protection.

- Using technology to exchange information on dedicated and encrypted platforms.

ISO 22396:2020 on the exchange of information between organisations

This ISO document acknowledges the evolution of the landscape of risk due to increased interconnectivity among private, governmental, and non-governmental organizations, leading to overlapping and boundary-crossing risks. It emphasizes the greater need for collaboration and information exchange to enhance resilience and security. Effective collaboration involves secure information sharing across both sectors to reduce vulnerabilities and improve organizational effectiveness. Challenges include defining coordination responsibilities and protecting sensitive business information. Successful information exchange can boost knowledge, enhance resilience, and provide additional benefits like increased access to restricted information and community building.

The Guidance document outlines principles, frameworks, and processes for establishing robust information exchange mechanisms.

It is applicable to private and public organizations that require guidance on establishing the conditions to support information exchange. As every ISO Guideline or Standard, it is IP protected and thus cannot be reproduced in this White Paper and needs to be purchased from National Standards Bodies or directly from ISO[9].

[7] *The Traffic Light Protocol (TLP) was created in order to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s).*

[8] *Joint Statement on the GDPR Implementation Report by 23 Organisations, including CoESS – see CoESS website's newsroom, position papers https://coess.eu/*

[9] *https://www.iso.org/standard/50292.html*

4. Mapping out of PPPs in Europe

In 2021, CoESS carried out a survey across 29 European countries, of which 24 are EU Member States. Only 9 countries reported having PPPs in place, namely: Belgium, Denmark, Finland, France, Germany, Italy, Spain, Sweden and the Netherlands. This survey was complemented by a further one a few years later under the EU-funded SAFE CITIES project [10]. This project aims to help to protect public spaces by providing a security and vulnerability **assessment framework** supported by an **interactive platform**.

CoESS is one of the partners of the large SAFE CITIES consortium, which brought together 16 partners from 9 countries, including universities, municipalities, LEAs, and ministries of interior.

Within this project, CoESS carried out a survey among its members, supplemented by desktop research to identify:

- Legal frameworks as a basis for PPPs in public spaces
- Tasks and competencies of companies
- Frameworks for PPPs
- Experiences with joint Security Vulnerability Assessments

As pointed out above, the PPPs and recommendations depend on the legal basis in each country, in particular whether PSCs are allowed to conduct tasks in spaces accessible to the public, and if so, which spaces and which tasks.

The key findings were that, where they existed, PPPs were usually part of formal frameworks, organised at municipality-level and of permanent nature including mostly:

- Points of contacts among LEA, PSCs and other actors (75%)
- Regular information exchange at management level (65%)
- Live information / data exchange in case of incidents (55%)

[10] https://safe-cities.eu/

The least used means of collaboration were:

- Pooling of resources (30%)
- Joint Vulnerability Assessments (17%)
- Joint trainings (10%)

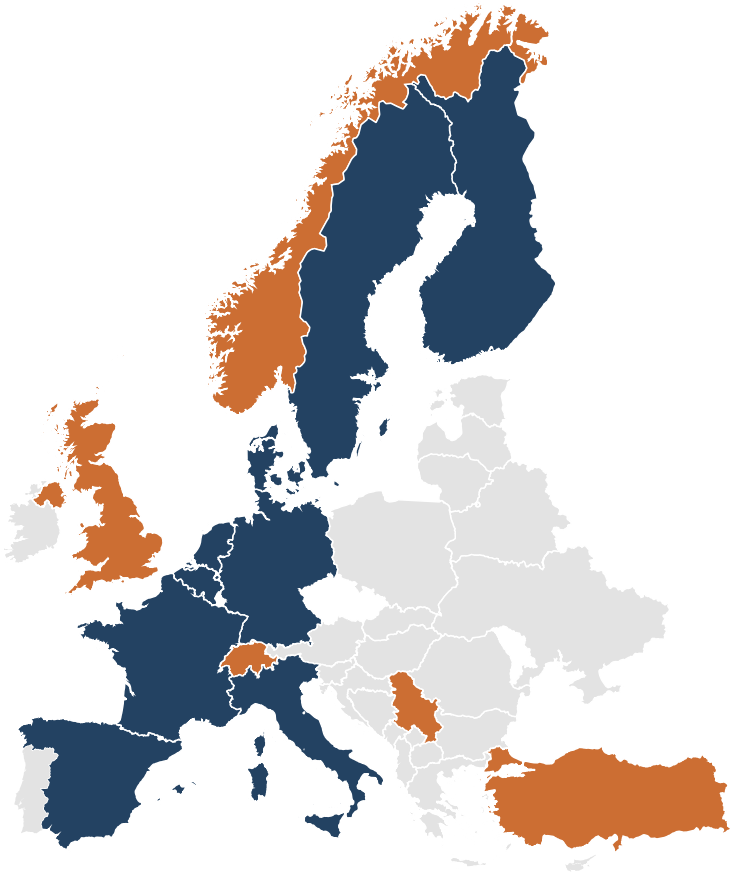
The main reason mentioned for this was the lack of trust for data sharing. Private security was often seen as late-entry enforcement service and respondents felt that the only way to change this was through trust-building and quality control.

Among the tasks that fall under PPPs in different countries we find the following:

- Where PSCs are allowed to provide services in spaces accessible to the public, this usually includes public events, as well as sports and festival facilities. Other public spaces covered include hospitals, asylum centres, public administration facilities, and recreation facilities such as parks or beaches. In the summer of 2024, PSCs worked in cooperation with the French LEAs to protect the Olympic Games in Paris.
- Several countries call upon PSCs to support the penitentiary system: perimeter surveillance, transport of detainees, guarding detainees in police stations.
- Aviation Security is also a domain mentioned in PPPs in Germany, whilst in other countries it is part of the tasks listed in the Private Security legislation.
- Public transport security is also mentioned as an area of PPP, as are transport hubs and ports, as well as the surveillance and protection of public buildings, military compounds or stations.

In Spain and Portugal, the law provides that private security have a special obligation to assist and collaborate with the Security Forces at their request, following their instructions in relation to the services they provide that affect public security or fall within their area of competence. Interestingly, out of the 5 non-EU countries surveyed, all reported having PPPs in place, namely Norway, Serbia, Switzerland, Turkey and the United Kingdom.

"In Spain and Portugal, the law provides that private security have a special obligation to assist and collaborate with the Security Forces at their request."



EU countries: PPPs in place

Non-EU countries: PPPs in place

5. Policy and Strategic Recommendations

Taking into account previous publications by CoESS, recommendations by the Commission, academic and other literature, and best practice examined in this document, below are areas where CoESS would recommend actions.

European Legislators:

- Revise the Public Procurement Legislation to guarantee bidders' compliance with Collective Agreements (where they exist) and to provide legal certainty for procurement authorities on the use of selection criteria related to qualitative working conditions, adequate training, and innovative services.

- Re-affirm the risk-based approach as the guiding principle in the interpretation and application of the General Data Protection Regulation (GDPR), e.g. through a targeted European Commission evaluation of Articles' 6, 9 and 23 interpretations in national law and a constructive dialogue between the regulator, data protection authorities, and the industry.

- Produce guidelines and recommendations for PPPs drawing from the best practice described in the White Paper.

National Legislators:

- Review Legislation: Examine existing laws to ensure they support effective and lawful PPP operations, removing legal barriers to information sharing and collaboration.

- Establish Clear Legal Frameworks: Define the roles and responsibilities of both public and private sectors in PPPs to ensure clarity and compliance.

- Promote Standardization: Encourage the development of standardized procedures for PPP operations to ensure consistency across different regions and sectors.

- The complementarity of LEA and PSC staff should be reflected in their respective training curricula and bridges between the two should be made possible.

Law Enforcement Agencies (LEAs)

- Enhance Training and Integration: Ensure that law enforcement personnel receive training on how to effectively collaborate with private security companies, including understanding the capabilities and limitations of private security.
- Regular Evaluations: Implement regular assessments of PPP effectiveness, making adjustments as needed to improve outcomes and maintain public trust.
- Information Sharing Protocols: Develop protocols that allow for safe, secure, and efficient sharing of information between public and private entities without compromising data protection standards.

Operators of protected spaces

- Vulnerability Assessments: Collaborate with both private security and LEAs to conduct regular vulnerability assessments of properties to identify and mitigate potential security risks.
- Clear Communication Channels: Establish and maintain clear lines of communication with security providers and LEAs to ensure rapid response and information flow during incidents.
- Invest in Security Infrastructure: Invest in advanced security technologies and infrastructure that can enhance the effectiveness of on-site security measures and support broader security efforts.

Private Security Companies (PSCs)

- Quality and Compliance: Ensure adherence to the highest standards of quality and compliance in all security operations to build trust and reliability with public partners and the community.
- Specialized Information: Provide relevant information to security personnel on public safety protocols, emergency response, and the specific security needs of the environments they protect.
- Technological Advancements: Invest in and deploy state-of-the-art security technologies that can complement public security measures and enhance the collective security posture.

“The complementarity between LEA and PSC staff should be reflected in their respective training curricula and bridges between the two should be made possible.”

6. Best Practice

This section describes a few examples of best practice in PPPs at different levels (national, regional or local), of different nature (formal frameworks, operational or punctual cooperations). Although we have tried to structure them along the same aspects, we do not have all information required to do this.

6.1. National Partnerships

The Red Azul and COOPERA Programmes – Spain

For almost a decade, LEAs have established cooperation programmes with the private security sector in their respective competence area, e.g. Red Azul[11] at the Policia Nacional and Programme Coopera at the Guardia Civil[12],all based on mutual exchange of information and reciprocity. Similar programmes exist at the level of the Basque and Catalan Forces.

The Red Azul Programme between the Spanish National and private security was launched in 2012 and establishes a model of professional collaboration of complementarity and co-responsibility, aiming at the pooling of resources, collaborative operational planning and the integration of information from private security into the intelligence system of the National. It transcends the current model of legal requirements and moves from the situation of the mere use of private security resources by LEA to a scenario of sharing of resources that imply the establishment of a true "security alliance" between private security and the National Police.

In its collaborative relationship with the Private Security Sector, the National Police assumes the following commitments:

- Reciprocity: On the part of the National Police and depending on the degree of relationship achieved in the collaboration (see further below), reciprocal information exchange and support will be provided as to what is necessary at all times for

[11] https://www.policia.es/_es/tupolicia_red_azul.php
[12] https://www.guardiacivil.es/es/servicios/seguridadprivada/colaboraseguprivada/plancoopera/index.html

the efficient fulfilment of the functions assigned to the private security services.

- Integration and distribution of information: The information from private security will be integrated into the intelligence system of the National Police, for exploitation by the competent Police Units.

- Participation in planning: In the operational planning of the National Police, the active participation of the services and capabilities of the private security service will be considered.

- Continuous improvement: The National Police takes into account any proposals to improve collaboration made by the private security sector.

On the other hand, PSCs who decided to participate in the collaboration programme with the National Police assume the following commitments:

- Use the procedures and channels provided by the National Police to carry out the different activities of collaboration.

- Make available to the National Police all information it has about criminal acts or events that may affect public security, corresponding to its area of competence.

- Comply at all times with its duty of assistance and collaboration, providing the National Police, both on its own initiative and at the Police's request, with the information and support that is necessary in the preventive and investigative areas.

- Make good use of the information received from the National Police, using it in the most appropriate way to improve citizen security and for the effectiveness and efficiency of private security service, and for the exclusive purposes for which it was requested and provided.

This collaboration fully respects what is foreseen by the legal framework in Spain, and is exclusively based on the needs in public security as well as mutual trust and loyalty.

For the exchange of information and operational support from the National Police to private security, the following elements must be met:

- The request made must be in accordance with the activity or function pf the PSC and necessary for the service.

- The request must have potential or interest for public security.

- The response will be limited to participating or executing what is truly relevant and appropriate to the request made.

The information that can be provided and received by the National Police within the Red Azul Programme will refer to the communication of security incidents and alerts, special events, execution of plans, detained, identified or searched persons, stolen or suspicious vehicles, criminal modalities, evolution of crime, information bulletins, reports, background checks and others of a similar nature that may benefit public security.

The information that is provided to private security by the National Police depends on the commitment reached between the two parties. An evaluation will be carried out based on the effectiveness and commitment of the PSC demonstrated with the National Police. Within this evaluation four degrees of collaboration exist - the first being the one with the least contribution of information and the last being the most thanks to the PSCs active and constant participation.

In concrete terms, the Red Azul Collaboration is organised into four Work Programmes:

1. MANAGE: This programme is administrative in nature and is aimed at PSCs, Departments and Offices. In this way, collaboration is encouraged and any operational needs or collaboration problems are mainly evaluated and detected.

2. OPERA: Operational programme, aimed essentially at business associations and unions, PSCs and Security Departments and detective offices.

3. INFORM: Communications programme aimed at the sector to provide general and specific information, depending on the area of action in question. It uses several tools to improve the distribution of information.

4. WATCH: This communication programme is aimed at private security officers and its purpose is to form a space for relationships with them. To access the programme, security officers have to enter among others their Professional Identity Card number.

With the implementation of the COOPERA Programme in 2010, the Spanish Guardia Civil has been making an effort, within the scope of its powers, to optimise its public-private collaboration with the security sector. Due to the maturity of the sector in Spain, it aims to integrate the private sector services, enhance public security capabilities, define data to be exchanged, as well as other approaches to guarantee a security continuum and the effectiveness of the collaboration. The Programme can be joined voluntarily by duly registered and licensed PSCs and consists of the following:

- Formal framework: The company signs a collaboration operating procedure. Institutional contact between the Guardia Civil and PSCs will be carried out at Manager level (centralised) and operational level (provincial level).
- Exchange of contacts: When joining the Programme, PSCs will provide the contact information of the Director or Security Manager who will act as interlocutor to the LEAs at management level, but also, if applicable, regional contacts and interlocutors to establish the operational level of the programme and the appropriate communication links down to the local level.
- Safe communication channels: the means of communication are regulated through the programme.
- Regular meeting forum: Coordinated groups meet at least twice a year at operational, and once a year at management, level. They are permanent bodies representing LEAs and PSCs, directed by the Guardia Civil, without prejudice to maintaining permanent contact.
- Information exchange: PSCs provide information on all those aspects that contribute to improve the fight against crime, for example on suspicious or criminal activities and complaints and modus operandi of criminal networks. Specific communication channels exist for urgent cases. LEAs provide information to PSCs on facts or circumstances that may affect the safety of private security personnel or the operation of its services, such as road closures and public order disruptions, serious criminal acts, fires and other disasters, and urgent threats. Such urgent information includes local situation reports, anti-terrorist prevention data and changes in the threat landscape, local or general protection and prevention plans, as well as operational information.
- Reporting: Joint reports are drafted by the Guardia Civil to create a common security culture while facilitating the preparation of risk analyses for entities participating in the programme on aspects related to security, and crime. They are based on open sources and data exchanged.
- Joint Training: the Guardia Civil coordinates joint training with different security services, both aimed at management and operational level.

Mille Occhi sulla Città – Italy

- Formal framework: The project, which literally means "A Thousand Eyes on the City" was launched in Italy in 2010 and the most recent agreement between stakeholders dates back to January 2022. The principle is that Private Security Officers, while exercising their duties, may observe and collect information useful for the police for the prevention and repression of criminal activities (including environmental crime). The Mille Occhi protocol establishes the framework and recommends that each Italian province implements the programme.

- PSC selection criteria: The police prefect identifies for each province the PSCs that shall be included in the project.

- Points of Contact: PSCs designate Single Points of Contact (SPOC) for the exchange of information.

- Regular meeting forum: A Technical Task Force (Tavolo Tecnico) is set up between the parties and is coordinated by the Central Direction of the Criminal Police, which promotes the standardisation of procedures and the use of technology.

- There is a regular evaluation of the protocol's implementation at province level.

- Exchange of information: The police may pass on information for research or alarm notices to PSCs as long as they don't breach the secrecy and confidentiality of data. The police can alert patrols to increase the number of operators able to check various situations.

PSCs shall report activities described in the list in the protocol:

- Suspicious persons or vehicles
- Flight from crime scenes
- Theft of car or motorcycle
- Children, elderly persons, people in a state of confusion or in difficulty
- Presence of obstacles on the streets
- Interruption of the delivery of energy sources
- Elderly persons having fled hospitals or other places where they undergo treatment
- Other situations where imminent crime is suspected
- Particular situation of urban degradation and social unrest.

- Training is delivered by the state for the interaction with the relevant public service and to carry out the observation activities with a preventive mindset. PS agents may also join other training or refresher training with the police.

- The Mille Occhi Milan protocol includes the following interesting provision: "The prefect may organise training for PSC agents with the support of Law Enforcement to encourage the professional growth and awareness of the responsibility and importance of the duties given to Private Security Staff".

- The costs of the technical means used and the training are borne 100% by the PSCs. This is explicitly mentioned in the framework protocol.

Project Griffin (now called ACT Awareness) – United Kingdom[13]

Project Griffin is a national counter-terrorism initiative designed by the National Counter Terrorism Security Office (NaCTSO) to safeguard cities and communities by educating businesses about terrorism threats, primarily from groups like DAESH (ISIL), Al Qaida, and their affiliates. Launched in April 2004 in response to the evolving terrorist threat highlighted by the attacks on September 11, 2001, in the United States and subsequent attacks in London on July 7, 2005, this initiative engages both public and private sectors to emphasize national security as a shared responsibility. Originally involving three major financial institutions in London, the initiative now encompasses a broader partnership between businesses, the City of London Police, and the Metropolitan Police. Project Griffin aims to help stakeholders understand the threat, guide actions during terrorist incidents, and enable the reporting of suspicious activities through briefing events led by trained police advisors. These events present various counter-terrorism awareness modules that enhance public and staff knowledge on how to mitigate and respond to potential terrorist activities, covering a range of threats from simple attacks to highly coordinated plots.

Project Griffin's mission is to involve community members in partnership with the police to deter, detect, and counter terrorist activities. It has been lauded for enhancing security awareness within the business community and facilitating intelligence sharing before, during, and after crises. Over time,

[13] https://www.gov.uk/government/publications/project-griffin

Griffin has expanded significantly, adapting to changing threats, notably from Daesh (ISIL), and is now the standard model for delivering counter-terrorism awareness and training across all police forces in England and Wales, and has also been adopted by Police Scotland.

The effectiveness of Project Griffin was notably demonstrated during the London bombings in July 2005 and other incidents, including a potential attack at the Tiger Tiger Night Club in 2007. Its success has led to its adoption in several countries, including Singapore, Australia, Canada, and the U.S., where it has been integrated into New York's Project Shield. Project Griffin exemplifies the power of strong public-private partnerships in enhancing community security and creating a challenging environment for terrorists, continually adapting to meet the evolving threat of terrorism.

Events are free and can last between one and six hours depending on the time available and number of modules covered. The modules are reviewed and updated regularly and currently cover the following topics:

- Introduction to Counter Terrorism
- Current Threat
- Identifying and Responding to Suspicious Behaviour
- Identifying and Dealing with Bombs (IED) and Suspicious Items
- Bomb Threats
- Responding to a Firearms and Weapons Attacks
- Document Awareness
- Drones - Unmanned Aircraft Systems (UAS)

An attendance certificate showing the modules covered is awarded to staff at the completion of each event, enabling business to monitor and evidence staff development and awareness.

As of 16 March 2018, Counter Terrorism Policing (CTP) moved all of its branded products under the ACT-Action Counters Terrorism banner, Project Griffin was one of those products and is now known at ACT Awareness, an e-learning platform.

6.2. Regional partnerships

Oslo: Guide to cooperation between the police and the security industry

The Guide, first published in 2015, is a joint publication of the Oslo Police District and the Norwegian Association for Services, NHO Service, which represents all services including private security. While some form of cooperation is still in place, the current situation is no longer as ideal as described below. However, because the Guide was comprehensive and considered a model for PPPs by CoESS, we are reproducing its key features below.

The Formal Framework

- The purpose of the Guide was to define the respective roles and responsibilities of the police and private security, provide solutions for a better cooperation, including practical elements, such as procedures and reporting forms.

- It comprises 3 main sections:
  - The framework and principles: responsibilities, duties, forms of cooperation, forums and the exchange of information. The target is the management level of both the police and private security.
  - Routines and procedures based on 3 different types of private security services: shopping centre security guards, urban environment security guards and bouncers. These were selected as they are the areas where police and private security mostly interact.
  - An explanation of how the intelligence and reporting forms shall be understood and used. This section also includes a feedback form for use in the cooperation meetings between police and the security industry.

Mutual understanding and knowledge:

- A generic description of the police, including policies and ranks, and of the private security industry is provided.

- Duties and legal framework are outlined for both police and security industry. For example, the use of force or the exercise of power and authority is explained.

PSC Selection criteria: Requirements to be fulfilled by security companies include legal compliance, the need to have a permanent contact point who can respond to notifications. PSCs must designate a decision-making participant who shall participate in the meeting. They must also provide feedback in the appropriate format and within a pre-determined deadline.

Exchange of Information

Regulations regarding the handling of information:

- The Guide recognises the need to share information and at the same time the limitations that the law sets in this respect. This generates frustrations from both sides. The Guide recommends that this should be addressed by the relevant authorities and political leaders.

- Legislation allows police to share information with security companies when necessary to support legal duties or prevent improper conduct, as outlined in the Police Register Act. The assessment should consider if sharing information enables better decision-making. For instance, police might have information about a security firm's employee with a drug issue, but must assess whether sharing is essential and proportional to the objective. Each case requires individual assessment, and information should typically be provided in writing, with electronic communication requiring encryption if confidentiality is needed. However, the evaluation revealed that most information exchanges currently happen verbally, with no electronic records shared due to legal constraints.
  - The handling of information in the security industry is governed by the Personal Data Act, which applies to both private and public sectors when electronic tools are used or information is in a register. The police, handling criminal cases, are exempt from this Act. Sensitive personal data requires a permit from the Norwegian Data Protection Authority and must adhere to strict handling rules. The security industry manages personal data for clients under data processing agreements, and can only process data as agreed in writing. While the police can share non-confidential information with security companies, these companies lack licenses to handle sensitive data from the police. This limitation hampers efforts to prevent and solve crimes, as the police are sometimes unable to share critical information with security companies. During the evaluation, several incidents have occurred in which the police held information about active criminal networks (images and vehicles) without being able to forward this information to e.g. alarm and security operations centres in vulnerable areas. This has made it difficult to prevent and avert planned criminal activity.
  - From the private security perspective, there may be limitations in the information it is able to share, as it handles classified information for a number of clients, and undertakes assignments at objects at where there is a statutory duty of confidentiality. Police may obtain such information if there is a court order.
  - The police significantly benefit from information provided by the security industry in criminal investigations, intelligence on incidents, and threat analysis. A problem-oriented approach and intelligence doctrine guide the Norwegian police's strategy, emphasizing cooperation with external partners. This collaboration is crucial for achieving an analytical and proactive working method, ensuring optimal use of police resources (Police Strategy 2010-2015).

- **Channel for the secure exchange of information**: The Oslo police operations centre has 20 phone lines, three reserved for the security industry, making it essential that operators understand

when to use each line, including the emergency number 112.

Regular meeting forum: Contact between security guards and the police operations centre: The police operations centre prioritizes registering information from security guards, as it may be the first report of an incident requiring police follow-up. To prevent unauthorized calls, a verification system requires security guards to contact the police through their monitoring centre, whichchecks their identity and assesses the situation before connecting them. Once connected, the guard provides a brief description of the incident. The security industry primarily uses lines for identity checks and general inquiries, with an alarm line for serious crimes. Security guards can also call the emergency number 112, where they will be asked control questions to verify the incident's legitimacy.

6.3. Operational and Local Partnerships

Spain: Protecting a Basque Police Station

Private Security Company performing access control of a Basque police station.

Below is a description of the tasks pertaining to this mission:

- Surveillance and protection of the property, as well as of the people who may be present, by conducting checks, patrols, inspections, and preventive actions as established for the fulfilment of their mission.
- Carrying out identity checks on individuals seeking to access the police station, addressing them in either Basque or Spanish depending on the language the individual wishes to use.
- Guards may refuse entry and record relevant information about the visitor (including ID number), purpose of the visit and destination within the station.
- Monitoring the vehicles parked in the exterior parking area designated for visitors, and managing access barriers.
- Performing initial inspections of all packages entering the premises.
- Conducting checks using the metal detector belonging to the Security Department on individuals wishing to enter the police station, as well as on their belongings, removing any items that are not permitted inside by regulation.
- Conducting random inspections of vehicles (including undercarriages and boots).
- Verifying, when necessary, alarms and any anomalies that arise at various points within the complex.
- Operating the CCTV systems installed at the police station:
- A system of cameras is arranged to monitor the perimeters of the police station.
- Continuous attention to the CCTV Control Centre.
- Monitoring the CCTV screens and operating the cameras, initiating the corresponding security protocols in case of incidents, as well as performing any other tasks that may be assigned in accordance with their regulatory responsibilities.
- Analysing and managing the received alarm signals (fire, storage, intrusion, etc.) and managing the technical resources at their disposal.

Belgium: Protecting Antwerp's Local Police

A similar agreement has been passed between the Antwerp local police and a private security company. This is a 7-year framework agreement, during which the PSC

secures the HQ of the Antwerp Local Police. Over the following years, the plan is to expand the locations.

- Missions include access control for visitors and managing the reception. Access control includes the use of technology, e.g. metal detector gates.
- The agreement provides that more services or solutions may be requested from the PSC, such as event security or support in operating technical equipment, such as drones and CCTV.

Police Zones of Mechelen-Willebroek/Belgium

Since the adoption of the new Belgian private security law in 2017, local authorities have gained greater clarity in using security companies for public space management. The Mechelen and Willebroek Police Zones, facing high crime rates since the 1990s, have leveraged this opportunity by developing a comprehensive public security action plan that emphasizes enhanced public-private collaboration. This is described in Prof. Dr. Marc Cools and Veerle Pashley from the University of Ghent in a 2018 publication[14].

One notable example is the consortium surveillance in the Mechelen industrial zone, where cooperation between the police and private security sector has proven successful.

Description of the PPP:

Private security services under a temporary contract include perimeter control with a permanent security presence, mobile patrols, and alarm-triggered interventions. The setup involves multiple partners—security companies, police, industrial zones, and government—coordinated through a municipal cooperation protocol. This consortium approach is cost-efficient, as the financial burden is shared among companies. While similar initiatives exist in Belgium, Mechelen-Willebroek was the first to implement such a model. Within this collaboration framework, security companies are required to report daily to the police. The new private security law also allows for the extension of such frameworks to other areas like shopping districts.

The Antwerp SHIELD Programme – Belgium

This public-private partnership in the field of counter-terrorism is described by Van Steden and Meijer in a paper on "PPPs in times of diffuse terrorist threat"[15] as best practice.

Formal Framework

The Antwerp SHIELD[16] programme serves as a comprehensive framework for a series of ongoing and forthcoming initiatives by the Antwerp Police Department, specifically targeting private sector security and counterterrorism efforts. This public-private partnership is founded on the principles of effective information sharing, aimed at bolstering security measures across the city.

The primary objective of the Antwerp SHIELD initiative is to facilitate seamless communication between the police and the private sector, thereby enhancing the police force's ability to combat terrorism and improve overall public safety in Antwerp. Drawing inspiration from the New York Police Department's SHIELD programme, which has long pioneered information sharing between the public and private sectors under the motto: "Countering terrorism through information sharing," Antwerp SHIELD aims to replicate this model. The NYPD SHIELD programme has demonstrated significant success in fostering regular, efficient communication with its members, and Antwerp SHIELD seeks to emulate this success to enhance security cooperation within its jurisdiction. Antwerp SHIELD offers training programmes for its members, providing a dedicated platform for education and skill development. These training sessions are available in various formats, including online tutorials and on-site workplace training. The courses, offered free of charge, equip participants with practical insights and strategies for identifying and responding to terrorist threats.

---

[14] *Cools, Marc, and Veerle Pashley. Private Veiligheid in Een Stedelijke En Gemeentelijke Context : Onderzoek Naar de Rol En Samenwerkingsmogelijkheden in Mechelen-Willebroek. Gompel&Svacina, 2018.*

[15] *Steden, R. van, & Meijer, R. (2018). Publiek-private samenwerking in tijden van diffuse dreiging: Een onderzoek naar diversiteit in werkwijzen en kansen in de Nederlandse en Vlaamse context. Den Haag: WODC.*

[16] *https://www.antwerpenshield.be/en/public-message/about-shield*

The Antwerp Diamond Quarter SHIELD implementation

One part of the SHIELD programme is the security of the Diamond district in Antwerp, where police, the municipality and several private security companies join forces to prevent unlawful acts. This project is frequently mentioned as a model of trust and respect between parties, as well as a high degree of satisfaction with the mutual information sharing. According to Van Steden and Meijer's research, this is mainly due to the Antwerp World Diamond Centre Security Office, which acts as an information broker between the stakeholders.

Exchange of information: The Security Office analyses and processes information, anonymizing confidential information where required and distributing it back to those who require it. The type of information includes geopolitical developments, suspicious situations or activities, threat assessments and camera footage.

Formal Framework, SPOCs and Regular Meeting Forum

The PPP is laid down in a safety protocol and a cooperation agreement and regular contact is maintained between the relevant stakeholders. The division of tasks, roles and responsibilities is clear to everybody, based on a written document.

Success factors

- Shared and mutual trust
- Stakeholders established as a team with Single Points of Contact within the various players
- Consensus on the approach for dealing with diffuse threats
- Sharing a sense of urgency
- Willingness to meet the others halfway

According to Van Steden and Meijer's research, this PPP checks all the success criteria mentioned in the literature on the matter.

The Netherlands – Teaming up to protect King's Day in Arnhem

The Netherlands has a long tradition of celebrating their sovereign, and since Willem-Alexander has acceded to the throne, King's Day has been celebrated on his birthday in April. It is celebrated in many cities, the centre of which turn into large event areas with around 200,000 people present. Royals traditionally go to several places to celebrate the day with their people. In 2009, there was a murder attempt with a car crashing into the procession. Eight people died at that event. This emphasizes the need to provide adequate protection for the event.

In the city of Arnhem, a PPP is in place whereby the Mayor, together with the local triangle (Mayor's office, LEAs and PSCs), provides for a safe event with fewer police officers, for example, during King's Day. According to the Mayor, in 2024, thanks to this PPP and the support of PSCs, 80 fewer officers were deployed in Arnhem than would normally be the case at a similar large event and can thus be deployed on other missions. In a newspaper article[17] about this cooperation, the Mayor declared that this allowed 2 police officers to dedicate 40 more days each to police investigations.

[17] *Gelderlander. (2024). "Een harde vuistslag in het feestgedruis, maar de dader wordt er in een oogwenk uitgepikt door Big Brother".*

CCTV allows for tracking any potential source of trouble without disrupting the scene and with good footage quality.

Event organizers are responsible for safety at their venues. The city assists with additional security or police if necessary. This allows for a quick and efficient response in case an incident occurs.

Services and solutions deployed:

- 2024 is the 3rd year that the city has put in place a joint command center equipped with screens displaying footage from various city cameras, manned by personnel from the city, police, medical services, fire department, enforcement, and private security companies. All services are coordinated as one unit under the command of the city's safety coordinator.
- The Team in charge of crowd management, preventing safety and security incidents and intervening when is necessary.

"According to the Mayor, in 2024, thanks to this PPP and the support of PSCs, 80 fewer officers were deployed in Arnhem than would normally be the case at a similar large event and can thus be deployed on other missions."

7. The International Security Ligue's Checklist for Building an Effective Private Security Partnership

"Careful selection and close monitoring has become more important as performance has improved: (a) because it has exacerbated differences in level of service one can receive; and (b) so that public agencies can take full advantage of the gains that the industry has made [18]."

[18] https://cdn.prod.website-files.com/6631523d581889857fab799d/6650ec62b1cb7134efa76d12_GovProcurementWP_Oct212020_Color.pdf *"Procuring and Managing Contract Security for Municipalities and Public Authorities - 10 Recommended Practices", The International Security Ligue, 2023*

Vendor Assessment Checklist: Questions to Review Before Work Begins			
	Yes	No	Details/Notes/Explanation
Part 1. Background, Structure			
Is the provision of security officers and services the provider's core business?			
Does the company demonstrate a sufficient level of expertise for the assignment?			
Does the security company have experience providing service in similar arrangements as ours?			
Is the company's operational and financial track record and reputation up to our standards?			
Has a background investigation revealed the absence of issues that could exclude the company from consideration (such as past fraud, corruption, violations, or other offences)?			
Is the company able to show that it meets insurance requirements?			
Has the company provided relevant financial records for the past three years?			
Does a financial review of the company indicate that it is financially healthy?			
Can the company demonstrate that it is current with all tax or other obligations?			
Has the company provided a list of customer references?			
Is there evidence that the company has successfully serviced a contract of similar size, structure, and responsibility?			
Has the company provided a list of similar sites where their guarding operations can be observed and inspected?			
Does the firm demonstrate an ability to provide the standard of service and level of expertise that we require?			
Has the company explained its security philosophy, and how that will be implemented in relation to our contract?			
Does a review indicate an absence of an unusual volume or pattern of complaints?			
Does an assessment indicate that the firm is proactive in ensuring their licensing is kept current?			
Is the company a member in good standing of recognized trade associations?			
Is the company clear of conflicts of interest or financial entanglements that would reflect negatively on us?			
Has the company received any industry awards or achieved membership in a selective industry group?			

Vendor Assessment Checklist: Questions to Review Before Work Begins			
	Yes	No	Details/Notes/Explanation
Part II. Personnel			
Is the company's existing management sufficient to support our operational requirements?			
Has the firm provided their average annual manpower and managerial staff over the last three years (comprising permanent, temporary and contract staff)?			
Does the basic training that the company provides to its security officers meet or exceed our specifications?			
Are we comfortable that the provider's commitment to inclusion and diversity in hiring will reflect positively on us?			
Are we comfortable with the level of expertise of the trainers that the company uses in its training and development programs (in-house or external trainers)?			
Does the company provide regular, refresher training to its officers?			
Can the company provide up-to-date records of staff training?			
Are the company's qualifications for security officers acceptable to us?			
Does the vetting that the firm's security officers receive meet our standard for background checks?			
Has the company shared an acceptable rate of annual staff turnover over the last three years?			
Is there evidence personnel meet any other skill requirements for duties under the contract (language skills, computer proficiency, etc.)?			
Is there proof that all specialized training necessary for personnel to carry out the requirements of the contract has been conducted?			
Will the guarding personnel that is assigned to our facilities be experienced in the type of work they will be performing?			
Can the company provide evidence that security officers are suitably fit for the work they are contracted to perform?			
Can the company provide a clear chain of responsibility as it relates to managing and servicing the contract?			
Is the outward appearance of contract personnel and equipment in keeping with our standards (uniforms, vehicles, etc.)?			
Do the skills and expertise of the company's management team suggest their ability to deliver excellent planning and service support?			
Has the company provided information about the skills and experience of each member of the management team and their responsibility within the contract framework?			
Are the skills and qualifications of the on-site manager suggestive that he or she can effectively carry out the contract?			
Are we satisfied with the skill and expertise of the contract manager?			

Vendor Assessment Checklist: Questions to Review Before Work Begins			
	Yes	No	Details/Notes/Explanation
Part III. Programs, Plans			
Is there evidence that the company's working conditions for guarding staff comply with all relevant legislation and/or collective agreements?			
Are the company's salary and benefit levels for its security personnel both sufficient and compliant with local union, state and/or national requirements?			
Do the company's safety policies and procedures meet regulatory requirements?			
Does the firm have a robust audit and quality assurance framework (ISO compliant, etc.)?			
Does the company have a robust corporate social responsibility program?			
Can the company provide evidence that it is committed to reducing health and safety risks to its security employees?			
Does the company have a code of conduct, integrity, or ethics program?			
Does the company have a policy addressing substance use that comports with our requirements?			
Is the supplier able to show that officers' working hours and shift patterns don't exceed good practices (for consecutive hours, days, sufficient breaks, etc.)?			
Is instruction on the company's ethics program provided to all its employees?			
Does a review of the company's customer invoices indicate that they are transparent and easy to understand?			
Can the company provide evidence of a suitable channel for managing complaints, feedback, and suggestions from its guarding personnel?			
Does the company have a career development or other career programs for its guarding personnel?			
Does the company have the relevant certifications necessary for the assignment?			
Does the company's operational plan for the contract include all necessary elements?			
Are the technology, tools, and equipment in the operational plan sufficient to provide service excellence?			
Does the company maintain an internal compliance and quality program?			
Are we satisfied with the company's plans and processes for protection of confidential information from disclosure?			
Does the provider's crisis management plan provide confidence that it will be able to assist us in a major disaster event?			
Have all verbal promises or representations made it into writing?			

Vendor Assessment Checklist: Questions to Review Before Work Begins			
	Yes	**No**	**Details/Notes/Explanation**
Part IV. Resources, Support			
Does the company have sufficient backup capacity, especially redundancies in key 24/7 operational infrastructure, to meet the requirements of the contract in an emergency?			
Does a review of the company's management structure and resources indicate an ability to respond to problems within required time frames?			
Is the company able to demonstrate that they have sufficient staff to effectively meets the requirements of the contract?			
Is the firm able to provide additional personnel support in a timely manner in the event they are required?			
Is the provider able to provide the equipment and training necessary to provide the services required in the contract?			
Are we satisfied with the additional or specialized training that the company can provide?			
Can the company outline its procedures for upholding the quality standards to which it commits?			
Are we satisfied with our recourse if a guard misses a shift?			
For all systems or equipment that the company provides in performance of the contract, can it demonstrate an ability to effectively operate and maintain the system?			
Are we satisfied with the company's use of technology to enhance officer performance?			
Has the company provided sufficient information about the support services it has available (such as administration, invoicing, etc.)?			
Are we content with the availability of supporting security and security-related services?			
Are we satisfied with the company's operational plan for monitoring the performance of the contract?			
Is the company's rostering methodology indicative of an ability to meet the contract's security requirements?			
Can the company show all required certifications associated with any technical equipment that will be used in fulfillment of the contract?			
If the company may use sub-contracted private security service personnel in certain instances, is there assurance that they also meet all quality criteria?			
Are the company's communication tools and systems adequate for the services required?			
Are we happy with the mechanisms the firm has in place to solicit our input, exchange information, and assess our level of satisfaction?			

7TH European Security Summit White Paper

POLICE

CoESS

Nederlandse Veiligheidsbranche

International SecurityLigue