



Position Paper

EU Baseline Preparedness Requirements

Brussels, 29 June 2026

The Confederation of European Security Services (CoESS) welcomes the European Commission's plan to develop EU baseline preparedness requirements. These requirements should help Member States keep critical infrastructure, essential services and civil protection systems functioning during crises, through strong public-private cooperation, workforce readiness and an all-hazards, whole-of-society approach. Private security must be adequately reflected in this framework.

Private security companies protect all types of critical infrastructure, including military perimeters, secure transport and logistics networks, safeguard publicly accessible spaces, operate Monitoring and Alarm Receiving Centres with alarm response services, provide aviation and port security, ensure secure cash services and protect supply chains. In a crisis, the industry may also support the protection of military transport and strategic logistics corridors. It is crucial to secure continuity in security services during a crisis, otherwise many other essential functions become more vulnerable. The sector is therefore not only a service provider, but an enabler of preparedness across the European economy and society.

CoESS therefore recommends that EU baseline preparedness requirements include the following:

1. Workforce availability

Member States should work with sectoral Social Partners to ensure that private security personnel remains available during crises, heightened alert or wartime. This should include workforce risk assessments, surge capacity planning, rapid mobilisation procedures and regular crisis-relevant training, so that critical infrastructure and essential services are protected under all circumstances.

2. Public support for preparedness investments

Member States should ensure that preparedness expectations for private operators are matched by clear cooperation frameworks. Crisis-ready capacity requires advance preparation, including specialised training and staffing arrangements. Where such capacities support public preparedness objectives, they should be reflected in public funding, contracts or other appropriate support mechanisms.

3. Operational status for security services

Member States should establish an appropriate operational status for security services, including their personnel and vehicles, to ensure service continuity. Where needed, such status should ensure access to critical resources, including fuel, electricity, telecommunications, protective equipment, vaccination or other public health measures. It should also prevent security workers from being unintentionally blocked by movement restrictions or border measures.

4. Legal protection of security personnel

Member States should ensure appropriate legal protection for private security personnel. Security officers protecting critical infrastructure, transport and logistic hubs, publicly accessible spaces or other essential services may face increased risks during crises. Their protection should reflect the public-interest role they perform, especially when they operate under emergency protocols or in support of public authorities.

5. Public-private crisis cooperation

Member States should involve private security in operational crisis planning, including joint training, emergency protocols, early-warning systems and secure information-sharing mechanisms. These structures should be created during peacetime. Early exchange of information on emerging threats helps public authorities and private operators react faster before and during crises. Monitoring and Alarm Receiving Centres operated by private security companies should be integrated into crisis communication, as outlined in our position on the [EU Critical Communication Systems Regulation](#).

About CoESS

CoESS acts as the voice of the private security industry, covering 23 countries in Europe and representing 45,000 companies with 2 million security officers. Private security provides a wide range of services for private and public clients, ranging from Critical Infrastructure to public spaces. CoESS is member of multiple EU Expert Groups and recognised by the European Commission as the EU employers' organisation representative active in EU Sectoral Social Dialogue with UNI Europa.

EU Transparency Register Number: 61991787780-18

Examples of Private Security Services in Europe

Private security services are part of the internal security framework of Member States and their regulation is a national competency. Responsibilities vary, but some services exist in all EU countries.

Protection of Publicly Accessible Spaces

Security services in public spaces involve the deployment of licensed, vetted security personnel and advanced surveillance technologies to monitor, deter, and respond to criminal activities and threats. These services work to enhance the security of publicly accessible spaces such as events and transportation hubs by maintaining a visible security presence, conducting patrols, and coordinating with law enforcement.



Critical Infrastructure Protection (CIP)

CIP services involve the deployment of security personnel and technology to protect essential facilities from threats like organised crime, terrorism and hybrid attacks. Such services ensure continuous operation of vital infrastructure by conducting risk assessments, monitoring for suspicious activities, and coordinating with public authorities to respond to potential incidents. They cover Critical Entities such as energy, healthcare and governmental facilities.



Remote Monitoring and Alarm Response

Remote monitoring and alarm response services are provided for a large range of clients, including Critical Infrastructure, supply chain facilities and other private premises. A Monitoring and Alarm Receiving Centre (MARC) is responsible for continuously monitoring security alarms and surveillance systems to detect and respond to potential security breaches or emergencies. It ensures timely communication with law enforcement and emergency services to manage and mitigate risks effectively.



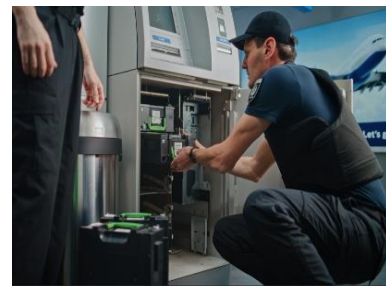
Aviation Security Services

Aviation security services protect passengers and their luggage, staff, aircrafts, air cargo and airport infrastructure against unlawful interference. They include access control, passenger and luggage screening, perimeter control, surveillance and guarding of security restricted areas, helping civil aviation stakeholders and air transport remain safe and secure during normal operations and during crises.



Cash-in-Transit and Cash Management

Cash-in-Transit and cash management services ensure the secure transport, processing and availability of cash for banks, retailers, ATMs and the wider economy. They protect cash as a safe and accessible means of payment, including during crises when digital payments may be disrupted and citizens need immediate access to money. These services are highly regulated due to security risks and are essential in maintaining public confidence, financial continuity and economic resilience.



Port and Maritime Security Services

Port and maritime security services protect ports, ships, passengers, cargo and maritime infrastructure (on- and off-shore) against unlawful acts and security threats. They include access control, screening, patrols, surveillance and guarding of restricted areas, helping ports remain safe, secure and operational as critical hubs for trade, energy supply, logistics and emergency response.

