NPSA Challenge Areas

Challenge Area	What this needs to enable
Vehicle Screening for Explosives, Weapons and Other Threats Vehicle screening for explosives, firearms and other mass-casualty threats often relies on expensive X-ray systems, manual searches or specialist detection capabilities. These approaches can be costly, time-consuming, resource intensive and difficult to deploy at scale. Current limitations may create problems at sites where rapid, efficient vehicle screening is required. Improved approaches are needed to enable fast, reliable and low-burden detection of threats in vehicles while maintaining operational efficiency and minimising disruption to drivers and passengers.	Rapid, low-cost vehicle screening that reliably detects threats intended to cause mass casualties or structural damage to buildings and infrastructure without invasive searches or ionising radiation.
Extended Reality (XR) for Protective Security Security tasks such as screening, searching and threat identification often depend on operator experience, training and sustained concentration. These activities can be time consuming and prone to variation in performance. Extended reality technologies offer opportunities to improve situational awareness, decision-making and operator effectiveness, but practical applications for protective security remain underdeveloped. There is a need to identify scalable, affordable ways to integrate XR into routine security operations to improve performance, reduce training burdens and increase confidence in security outcomes.	Practical, low-cost XR applications that enhance security operations, decision-making and workforce effectiveness.
Low-Compliance Crowd Screening for Concealed Threats Current security screening processes often require individuals to actively participate in checkpoint-based searches, creating friction, queues and operational overhead. For busy venues and events, these approaches can affect visitor experience and limit screening coverage. Security operators require more	Unobtrusive screening of moving crowds for concealed threats while maintaining efficient visitor flow.

effective ways to detect concealed threats within moving crowds while maintaining efficient entry and minimising disruption. Enhanced screening capabilities could improve security outcomes while supporting smoother, less intrusive access to public and private venues.	
Public Warning of Hostile Vehicle Attacks Hostile vehicle attacks can develop rapidly, leaving little time for people to recognise and respond to danger. In locations where permanent or temporary hostile vehicle mitigation measures are not feasible, there may be limited means of alerting people to an approaching threat. Improved capabilities are needed to rapidly detect, verify and communicate imminent vehicle threats to people in the vicinity, helping reduce harm and improve public safety.	Rapid detection and local warning of hostile vehicle threats to support immediate public action.
Device-to-Vehicle Data Blocker Assurance Connecting mobile devices to vehicles can result in transfer of personal and operational data to vehicle systems, potentially exposing sensitive information through servicing, resale, telemetry services or unauthorised access. While data blockers designed to enable mobile device charging exist, assurance that they fully prevent data transfer remains challenging particularly for USB-C connections. Organisations require reliable methods to validate that data blockers eliminate all unintended communications between devices and vehicle USB-C ports, reducing the risk of data leakage while maintaining safe charging functionality.	Reliable assurance that data blockers prevent all unauthorised device-to-vehicle data transfer via USB-C ports.
Secure Device-to-Vehicle Connectivity Modern vehicle connectivity features often require mobile devices to share data with infotainment systems, creating risks that personal or operational information may be stored within vehicle systems. This can expose data during servicing, hire, resale or compromise of the vehicle. Current solutions	Secure device-to-vehicle connectivity that preserves functionality without storing user data in vehicles.

may require trade-offs between functionality and security. Improved approaches are needed that allow users to access vehicle microphones, speakers and interfaces without transferring sensitive data to vehicle systems.	
Detection of Camera Use Hostile reconnaissance is often a precursor to attacks, with photographs and video providing valuable information for planning and target assessment. Current methods for identifying people capturing imagery typically rely on operator observation or limited automated detection tools. This can make reconnaissance difficult to identify consistently, particularly across large or complex sites. Improved approaches are needed to detect and understand photography activity, helping organisations identify potential threats earlier and take appropriate preventative or investigative action.	Reliable detection of hostile reconnaissance through identification of photography and video activity.
AI in Training – Incident Response Simulations Immersive and simulation-based training can significantly improve preparedness for rare but high-impact security incidents. However, developing realistic, site-specific exercises is often expensive, resource intensive and difficult to scale. Many organisations lack the capability to repeatedly test incident response procedures, control room operations and team coordination in realistic environments. More accessible approaches are needed to creating and delivering adaptable, high-quality site-specific simulation training that supports continuous learning, team development and organisational preparedness at low cost.	Scalable, affordable and site-specific incident response training through realistic simulation.
Baselining and Monitoring AI Capability As AI becomes increasingly embedded within security technologies, understanding and maintaining system performance throughout deployment becomes more challenging. AI-enabled systems may adapt over time, potentially affecting accuracy, consistency and	Continuous assurance that AI-enabled security systems remain effective, reliable and trustworthy over time.

reliability. Performance degradation can result in missed security events, excessive false alarms and reduced user confidence. Organisations require effective approaches to establish performance baselines and continuously monitor system effectiveness, ensuring security capabilities remain reliable, transparent and fit for purpose throughout their operational lifecycle.	
Wide Area Monitoring While mature technologies exist to protect site perimeters, detecting and tracking intruders across large, complex or cluttered sites remains challenging. Existing solutions can struggle to provide consistent coverage without generating excessive false or nuisance alarms. These limitations can reduce situational awareness and increase the burden on security teams responding to potential incidents. Improved monitoring capabilities are needed to reliably detect, track and assess intrusions across wide areas while maintaining operational efficiency and minimising false alerts.	Reliable wide-area detection and tracking with low false-alarm rates across complex sites.