



Home Office Challenge Areas

Home Office Mission – Public Safety

Challenge Area	What this needs to enable
Digital evidence: capture, triage and insight at scale: Policing and law enforcement partners need to capture, process, analyse and interpret digital evidence at the pace and volume required.	Improved data management and exploitation into actionable intelligence and more timely investigative insight.
Policing public contact and victim experience: increasing confidence and engagement: The delivery of consistently high-quality public contact and victim support that keeps people engaged through reporting, investigation and justice processes.	Improved victim confidence and trust in policing, leading to higher reporting rates, stronger engagement throughout investigations, reduced case attrition, and more effective safeguarding and justice outcomes.
Improved data sharing between policing and partners: Fragmented data sharing limits the ability to identify patterns, connect risk, and coordinate effective multi-agency action.	Secure, efficient, standardised data sharing across forces; better integration for insight generation.
Online harm and exploitation: Approaches to keep up with the scale and evolution of online sexual offences (including child exploitation) and technology-enabled abuse.	Prevent, detect and investigate technology enabled crimes effectively and at speed.
Future-facing policing capability: As crime and risk shift into digital and “smart” environments, policing must adapt culture and systems to embrace new technologies and enhance their capability.	A workforce that is digitally-enabled and empowered for example, improved cyber investigation/prevention; workforce safety; operational mobility and embedded innovation/strategic foresight.

Home Office Mission – National Security

Challenge Area	What this needs to enable
Lawful access and investigatory capability in a rapidly evolving tech environment: Rapid technological advances including in encrypted communications, decentralised platforms and new data architectures are reducing the ability of law enforcement and national security partners to access intelligence.	Sustainable lawful access capabilities that keep pace with technological change; scalable solutions for accessing, processing and analysing otherwise inaccessible telecommunications data; alignment of technical capability and legal frameworks.
Scale and sophistication of cyber and economic threats outpacing response: Cybercrime, fraud and financially enabled crime continue to grow in scale and complexity, challenging the ability of current systems to detect, disrupt and recover losses.	Improved detection and disruption capabilities, stronger partnerships with the private sector, enhanced asset recovery approaches, and scalable cyber resilience across sectors.



Complex and hybrid threats from state actors: State actors are employing increasingly integrated approaches spanning a range of mechanisms including cyber, espionage, influence, and economic tools.	Whole-system resilience through connected capability development strengthening protective security across sectors, and continued, improved coordination across government, industry, academia and with international partners.
Evolving UK threat landscape: The UK faces a diverse and evolving range of high-impact threats, including those employing complex or coordinated methodologies such as terrorist use of explosives, unmanned aerial systems (drones), and chemical, biological, radiological and nuclear (CBRN) materials, alongside the potential for multi-site or novel attack vectors. This necessitates continued enhancement of protective security, preparedness, and whole-system response capabilities.	Enhanced protective security and preparedness across sectors, improved cross-agency interoperability and response to a range of threat types, and enhanced recovery capability to support communities following incidents.
Emerging threats outpacing legislative and policy frameworks: Existing legislation and policy frameworks must adapt to technological innovation and evolving threat methodologies.	Agile policy and legislative development, anticipatory horizon scanning, and frameworks that allow rapid adaptation to emerging threats while maintaining safeguards.

Home Office Mission – Borders and Migration

Challenge Area	What this needs to enable
Adaptability and evolution of organised immigration crime: Methods evolve rapidly and continuously change challenging the ability of law enforcement to counter and stay ahead of the threats posed.	More effective deterrence and disruption strategies, improved understanding of criminal business models, and coordinated interventions, particularly to limit financial and communication enablers.
Balancing border security, flow efficiency and public confidence: The border system must simultaneously enable legitimate movement and detect threats, but faces challenges in technology adoption and public perception.	Advanced border technologies, enhanced risk-based decision-making, leading to stronger public confidence in border security performance.
Integration and long-term outcomes for refugees: Barriers to employment, services and social integration limit outcomes for refugees and reduce their long-term contribution to the UK.	More effective, joined-up integration support, improved access to employment and services, and better understanding of long-term outcomes and impacts.