Header page

Freeports security and illicit activity guidance

To assist the Freeports in managing potential security risks, of **all** of the businesses located **within and around** their sites (as per commitments in your Memorandums of Understanding), a range of tools and guidance is available:

- Suggested approaches to risk reports and security plans
- Protect and preparedness advice and guidance from National Counter Terrorism Policing
- HMRC guidance
- Home Office and Department for Transport guidance
- Cyber security

Suggested approaches to risk reports and security plans

A potential approach to producing the Risk Report

1. Threat identification and assessment – identify the types of threat and determine the likelihood of each occurring and the possible impact on the Freeport sites.
2. Vulnerability assessment – determine what the key assets are and how they can be exploited, examine the security measures in place and their effectiveness and consider residual weaknesses.
3. Risk assessment of residual risks – assess the probability of an attempt and the likelihood it may succeed (the residual risk). Produce Risk Register.
4. Recommendations for risk management – make recommendations to your Freeport Security Group to effectively and efficiently address weaknesses and mitigate identified residual risks.
5. Review Risk Report – review Risk Report at least every six-months, when specific intelligence is received on a particular threat, when new information becomes available and when there is a major incident. This may include testing and exercising of the policies and processes are in place, as appropriate.

Security Plan - Key Steps that Freeports could follow

1. Determine roles and responsibilities
2. Develop the terms of the plan
3. Agree monitoring arrangements
4. Ensure Unanimous Agreement
5. Finalise the document
6. Review and amend the plan (at least annually)

NCTP page(s)

Protect and Preparedness advice and guidance from National Counter Terrorism Policing

Websites for advice and guidance on a wide range of security topics

- **ProtectUK -** provides free advice, guidance and learning to help businesses and communities understand protective security and improve their response to the risk of terrorism.
- **National Protective Security Authority** (NPSA) - the UK government's National Technical Authority for physical and personnel protective security.

Free Awareness Products to upskill staff and stakeholders to make them aware of the potential threats

Threat Levels - threat levels are designed to give a broad indication of the likelihood of a terrorist attack

ACT eLearning – entry level award winning ACT e-Learning. Topics include an introduction to counter terrorism, identifying security vulnerabilities, identifying and responding to suspicious activity and how to respond to a firearms or weapons attack.

ACT Security e-Learning - specialised training for front line security operatives.

See, Check and Notify (SCaN) - See, Check and Notify (SCaN) aims to help businesses and organisations maximise safety and security using their existing resources. Your people are your biggest advantage in preventing and tackling a range of threats, including criminal activity, unlawful protest and terrorism.

Risk Management

Visit the ProtectUK **risk assessment** tool for step-by-step guidance to help you carry out vulnerability assessments.

Once you have identified vulnerabilities, consider the options recommended on the PROTECT:UK Risk Management Controls List.

Venues and Public Spaces Guidance

Venues and Public Spaces (VAPs) guidance - provides protective security advice in a number of sectors and scenarios. It has been developed through extensive research and analysis of previous incidents, and the assessment of current known threats. It covers the key forms of protective security: physical, personnel, cyber and personal, and helps give guidance on how different sectors can act to help make their businesses, institutions or organisations safer. There is additional guidance on evacuation, invacuation, lockdown and protected spaces. This will help you understand how to keep people safe when an incident is taking place and how you might communicate it.

Testing and Exercising

ACT in a Box - digital interactive tool that enables businesses and voluntary organisations to rehearse and explore their response to a terrorist incident as a group in a safe-to-fail environment.

You should also consider what testing and exercising you should do on your own site to test your plans and people, and what opportunities there may be locally. E.g. stakeholder groups / blue light services etc.

Toolkits - Resources to help further enhance your security posture

CT / Crime Crossover Toolkit - guidance is available to help them consider and adopt measures that will keep your facilities safer from both crime and terrorism.

National Stakeholder Menu of Tactical Options - a set of options which can be used by the private sector and security industry to enhance the wider national security posture at times of raised threat or in response to a terrorist incident.

Security Minded Communications - Security-Minded Communications (SMC) is designed to disrupt hostiles and to make a hostile believe that if they were to choose your organisation or event as a place to attack, they will almost certainly fail.

Vigilance toolkits - Counter Terrorism Policing is encouraging organisations, venues and events, to play their part in helping to keep everyone safe. An Action Counters Terrorism (ACT) vigilance campaign toolkit is available on ProtectUK website in various forms.
Security on your Side - a newly developed Security Minded Communications (SMC) campaign designed to amplify the deterrent effect of Hostile Vehicle Mitigation (HVM) measures.
Think Before You Link (TBYL) - allowing users of social media and professional networking sites, such as LinkedIn and Facebook, to better identify the hallmarks of fake profiles used by foreign spies and other malicious actors.

CCTV

Control Rooms - guidance that links the fundamental principles of Deter, Detect and Delay and how these can be provided by a well-run control room. NPSA also offer a CCTV operators course, simulating multiple terrorist situations and enable delegates to practice decision making in real time.

Guidance from the National Protective Security Authority

National Protective Security Authority (NPSA) - the UK government's National Technical Authority for physical and personnel protective security.
Passport for Good security - for Senior Executives. It sets out the key themes for best practice and provides relevant prompts for the actions you need to take as part of your strategy. It will help to identify, assess and mitigate the threats to your organisation
Catalogue of Security Equipment - The Catalogue of Security Equipment (CSE) is available to help security practitioners to identify appropriate physical security equipment. The CSE provides a range of products that have been evaluated against specific NPSA security standards and the performance rating achieved.
Build it Secure – guidance got how to incorporate security principles throughout the build lifecycle. This includes information management, governance, risk management, operational requirements and security deliverables.
Building and Infrastructure – what measures can be used around the perimeter.
Security-Minded approach to developing Connected Places - Guidance on how to take a security-minded approach to developing, managing and maintaining connected places
Secure Innovation – advice and guidance for business start-ups.
Supply Chain Security Guidance – separate guidance for business leaders / practitioners / suppliers
Secure Business - Supporting business leaders to operate securely with overseas parties
Personnel and People Security comprises an integrated set of policies, procedures, interventions and effects which seek to enhance an organisation or site's protective security

From RIBA: Security Overlay to the RIBA Plan of Work - for everyone involved in the safe and secure design, construction and operation of any building. A valuable industry document to support better long term security outcomes for everyone involved in the lifecycle of a building.

HMRC page

HMRC Freeport guidance

- Report tax fraud or avoidance to HMRC - GOV.UK
- Whistleblowing for employees: What is a whistleblower - GOV.UK
- Tax avoidance schemes aimed at contractors and agency workers - GOV.UK
- Corporate offences for failing to prevent criminal facilitation of tax evasion - GOV.UK
- How to spot missing trader VAT fraud
- Supply chain due diligence principles - GOV.UK
- Check for signs of labour fraud in construction - GOV.UK (www.gov.uk)
- Check for signs of payroll company fraud - GOV.UK (www.gov.uk)
- Mini umbrella company fraud - GOV.UK (www.gov.uk)
- Help with labour supply chain assurance — GfC12 - Examples - Guidance - GOV.UK
- Tell us about suspicious activity that may be linked to money laundering - GOV.UK
- Your responsibilities under money laundering supervision - GOV.UK

Customs sites

- Due diligence when making customs declarations - GOV.UK
- Report tobacco or alcohol tax evasion - GOV.UK
- Report smuggling - GOV.UK
- Registered dealers in controlled oil (Excise Notice 192) - GOV.UK
- How to make due diligence checks for Plastic Packaging Tax - GOV.UK
- Carry out checks and keep records if you're approved for FHDDS - GOV.UK
- UK strategic export controls - GOV.UK
- Export controls: military goods, software and technology - GOV.UK

Home Office page

Home Office and Department for Transport guidance

- Threat and Risk Assessment
- The national maritime security programme
- Maritime security training aids - GOV.UK - security training for port personnel.
- International Ship and Port Facility Security Code (The International Maritime Organisation)

Cyber page

Cyber security guidance

- National Cyber Security Centre - NCSC.GOV.UK
- Small Business Guide (for small businesses)
- 10 Steps to Cyber Security (for medium/large organisations)
- Active Cyber Defence
- Supply Chain Security Guidance
- Incident Management
- Report a Cyber Incident to the National Cyber Security Centre (We also recommend contacting the police to report a crime)
- England and Wales: Reporting fraud and cyber crime | Action Fraud

Scotland:

- Protecting yourself against cybercrime - Police Scotland
- Cyber Incident Response Toolkit
- SC3 Threat Reports