



Guide to UK Regulators

Physical and Cyber Security

Rural Estate &

Critical National Infrastructure

Energy, transport, communications, water, nuclear and food networks, onshore and offshore, and the farms, estates, heritage sites, woodlands and rivers that host or depend on them

Produced by: Rural SafeGuard (Frank Cannon CSyP)

Date: 18 September 2026

Revision: 1

IMPORTANT NOTICE

This guide is produced by Rural SafeGuard for general information purposes only. It is not intended to be, and should not be relied upon, as, a definitive or complete statement of the law, and it is not a substitute for independent legal advice. Rural SafeGuard does not accept any liability for any action taken, or not taken, in reliance on the information contained in this guide. Operators, owners and occupiers of critical national infrastructure, and the farmers, growers and landowners who host or depend on it, should seek independent legal advice before taking any action in reliance on the regulatory arrangements described here. Legislation, regulator guidance and the parliamentary Bills referred to in this document may change after publication; readers should check current requirements at legislation.gov.uk, bills.parliament.uk and the website of the relevant regulator.

Contents

Contents	2
1. Bottom line up front	3
1.1 Regulator-by-network summary	4
1.2 Changes to watch (as at 18 September 2026)	6
2. Purpose and scope	8
3. How UK critical national infrastructure security regulation is organised	9
3.1 The 13 critical national infrastructure sectors and Lead Government Departments	9
3.2 The three National Technical Authorities	9
3.3 The cyber security regulatory model: Network and Information Systems Regulations 2018	9
3.4 The physical security model	10
4. Cross-cutting national bodies	11
5. Food, farming and fisheries: the farm-to-fork chain	13
5.1 Regulators and authorities across the chain	13
5.2 Agricultural technology, connected machinery and the Agricultural Engineers Association	16
5.3 Where the gaps are	17
6. Scrap metal, waste, heritage and freight crime	19
6.1 Scrap metal dealers and metal theft	19
6.2 Waste management, waste crime and fly-tipping	20
6.3 Heritage crime: places of worship and national heritage sites	22
6.4 Freight and transport crime: cargo theft on road, rail, air and sea	23
6.5 What this means for rural estates	25
7. Rural land uses and rural crime regimes	27
7.1 Construction sites, plant theft and remote energy sites	27
7.2 Car boot sales, markets and events on private land	28
7.3 Forestry, woodland and timber	29
7.4 Rivers, angling and inland fisheries	30
7.5 Wildlife, livestock, horses, pets and firearms	31
7.6 Rural crime governance and the bodies that count it	32
8. Energy networks	34
8.1 Electricity (transmission, distribution, generation, interconnectors, system operation)	34
8.2 Gas (downstream transmission, distribution, storage, liquefied natural gas terminals)	35
8.3 Oil and upstream gas, including offshore production, pipelines and fuel supply	35
9. Civil nuclear	36
10. Transport networks	37
10.1 Rail (mainline, light rail and metro, Channel Tunnel)	37
10.2 Road (strategic road network, tunnels, traffic control and intelligent transport systems)	37
10.3 Aviation and space	38
10.4 Maritime, ports and shipping	38
11. Communications and digital infrastructure	39
11.1 Telecommunications networks and services	39
11.2 Subsea cables and undersea infrastructure	39
11.3 Digital infrastructure, data centres and digital services	40
12. Water and wastewater networks	41
13. Other critical national infrastructure sectors	42
14. The offshore dimension: territorial waters, the UK Continental Shelf and the Exclusive Economic Zone	44
15. Bibliography	45

1. Bottom line up front

This guide is written for the organisations that work alongside Rural SafeGuard to reduce the rural crime risk: insurers, farming and landowning bodies, trade associations, police and crime commissioners, rural crime police units and the professional security sector. It answers one question for every network and land use it covers, namely who regulates it, who polices it and who counts the crime against it, and in doing so it frames a problem statement.

Food is one of the thirteen critical national infrastructure sectors, yet the agricultural and food-producing sectors have none of the cyber and physical safeguards that every other sector has been given. That gap sits at the centre of the national debate on food security, homeland defence and rural resilience, and closing it is the collaborative task this guide is intended to support.

The unregulated ground comes first. Section 5 covers the farm-to-fork chain: no statutory security regulator, no place in the Network and Information Systems regime or in the Cyber Security and Resilience Bill, no product security requirement on the connected machinery, robotics and sensors that farming now runs on, and a National Audit Office finding in September 2026 that the Department for Environment, Food and Rural Affairs has not engaged sufficiently with industry on the resilience of the food supply chain.

Section 6 covers the crimes that reach the rural estate through its end markets and its supply lines: scrap metal, waste and fly-tipping, heritage and places of worship, and freight in transit. Section 7 covers the rural land uses that share the farm's exposure: construction sites and plant, remote solar, wind and battery installations, car boot sales and markets, woodland, rivers and fisheries, wildlife, livestock, equine, pet and firearms law, and the national bodies that set rural crime policy and count its cost.

The pattern across all three is the same: almost every asset is regulated for safety, planning, animal health, conservation or licensing, and almost none for security; no statutory security duty falls on the owner; the national policing units are small, grant-funded and in several cases paid for by the industries they protect; and police recording cannot separate rural, freight, heritage or plant crime from general theft, so the figures that shape policy come from insurers and industry bodies.

The regulated benchmark follows. Sections 8 to 14 describe the energy, nuclear, transport, communications, water and other designated networks that cross or sit on rural land, onshore and offshore. Each has a Lead Government Department accountable for its protective security, a statutory cyber regime under the Network and Information Systems Regulations 2018 with a named Competent Authority, incident reporting, inspection and penalties, and either a dedicated physical security regime or Lead Government Department oversight backed by National Protective Security Authority advice. The Cyber Security and Resilience Bill, expected to receive Royal Assent late in 2026, will widen and tighten that regime and carries a power to add sectors by regulations.

These sections are the evidence that the model exists, works and could be applied to food and farming: the same architecture of a responsible department, a competent authority, a security standard and a reporting duty.

For the organisations reading this guide the ask is therefore twofold.

- First, to collaborate in lobbying the right people: the Department for Environment, Food and Rural Affairs as Lead Government Department for food, the Department for Science, Innovation and Technology which holds the Bill's power to add sectors, the Home Office on rural crime recording and the funding of the national units, the National Police Chiefs' Council on its rural and wildlife crime strategy, and the manufacturers' and farming bodies on secure-by-design equipment.

- Second, to press for the stakeholders in the agricultural and food-producing sectors to be mandated to apply the same good governance that the regulated sectors already apply, rather than leaving it to insurer conditions and voluntary schemes.

In the meantime the practical conclusions are consistent throughout: report to the licensing authority as well as the police, write accredited standards into contracts and leases, mark and register everything that can be marked, and give the industry bodies the incident data that lets them make the case.

The table at Section 1.1 names the principal regulators for each land use and network and points to the section containing the full detail; Section 1.2 lists the regulatory changes in progress as at 18 September 2026.

1.1 Regulator-by-network summary

Network	Principal security regulators	See Section
All sectors — advice	NCSC (cyber), NPSA (physical/personnel), UK NACE (technical), Counter Terrorism Policing/Counter Terrorism Security Advisers (CTSAs).	3.2, 4
All sectors — premises	Security Industry Authority (SIA) under Martyn's Law (premises duties expected spring 2027) for qualifying premises (200 or more people expected at the same time, including shops and food premises) and events (800 or more).	4
Food, farming and fisheries (farm to fork)	No statutory security regulator. Defra (LGD), Food Standards Agency (FSA)/Food Standards Scotland (FSS) and National Food Crime Unit, Animal and Plant Health Agency (APHA) (biosecurity), Marine Management Organisation (MMO) and devolved fisheries bodies, Border Force and port health authorities, HSE/Home Office (inputs); Office for Product Safety and Standards (OPSS) (consumer connectable products only); Agricultural Engineers Association (AEA) (machinery trade body, advisory); NCSC/National Farmers' Union (NFU) advice; police rural crime units.	5
Scrap metal and metal theft	Local authorities (Scrap Metal Dealers Act 2013 licensing, England and Wales; Civic Government (Scotland) Act 1982 in Scotland; no equivalent in Northern Ireland); police and British Transport Police (National Infrastructure Crime Reduction Partnership); Opal; Home Office.	6.1
Waste crime and fly-tipping	Environment Agency, Natural Resources Wales, Scottish Environment Protection Agency, Northern Ireland Environment Agency (permitting, Joint Unit for Waste Crime); local authorities (fly-tipping fixed penalties, vehicle seizure); Defra; police (Crime and Policing Act 2026 penalty points).	6.2
Heritage crime, places of worship and heritage sites	No security regulator. Historic England / Cadw / Historic Environment Scotland / Department for Communities (NI) with local planning authorities (consent offences); police and Crown Prosecution Service (ARCH memorandum); Home Office faith-site security funding; Security Industry Authority (Martyn's Law standard tier for worship).	6.3
Freight and cargo crime	No lead body or offence. Police forces (theft from vehicle); industry-funded NaVCIS Freight; Opal; NPCC vehicle crime lead; Home Office (policy; freight crime flag pilot); DfT (lorry parking). Statutory cargo security only for air (CAA regulated agents and known consignors), rail (NRSP) and ports (ISPS). TAPA standards voluntary.	6.4
Construction sites, plant theft and remote energy sites	HSE (site safety only); police; NCATT (industry-funded, Northumbria Police); CITS and CESAR; Equipment Theft (Prevention) Act 2023 regulations awaited. Solar, wind and battery sites unregulated for security unless NIS-designated.	7.1
Car boot sales and events on private land	No licence in England, Wales or NI; planning 14-day limit, market rights, Trading Standards, food registration. Scotland: council market operator's licence (includes car boot sales) and second-hand dealer licensing.	7.2
Forestry and timber	Forestry Commission / Scottish Forestry / NRW / Forest Service NI (felling licences, unlimited fines since 2023); OPSS (UK Timber Regulation); police (timber and plant theft).	7.3

Network	Principal security regulators	See Section
Rivers and inland fisheries	Environment Agency and NRW (rod licences, byelaws, enforcement officers) with the Angling Trust; District Salmon Fishery Boards (Scotland); DAERA and Loughs Agency (NI); police (fish theft, poaching).	7.4
Wildlife, livestock, horses, pets and firearms	Police with NWCU and NRCU; APHA/RPA (identification); Defra (equine database); chief officers of police (firearms licensing, Home Office guidance). PCSC Act 2022 hare coursing offences; Dogs (Protection of Livestock) (Amendment) Act 2025 in force 18 March 2026; Pet Abduction Act 2024.	7.5
Rural crime governance	NPCC Rural and Wildlife Crime Strategy 2025–28 (DCC Nigel Harrison); NRCU and NWCU (Home Office grants); National Rural Crime Network (PCCs); NFU Mutual Rural Crime Report (£41.5m in 2025).	7.6
Electricity (GB)	Cyber: Department for Energy Security and Net Zero (DESNZ) + Ofgem (Network and Information Systems (NIS)). Physical: DESNZ (Lead Government Department (LGD)) with National Protective Security Authority (NPSA); Ofgem licence conditions.	8.1
Energy — Northern Ireland	Cyber: Department of Finance (NI). Economic: Utility Regulator. LGD: Department for the Economy (NI).	8.1, 8.2
Gas downstream (GB)	Cyber: DESNZ + Ofgem (NIS). Physical/integrity: Health and Safety Executive (HSE); DESNZ.	8.2
Oil and upstream gas incl. offshore	Cyber: DESNZ (NIS). Physical/safety: HSE Energy Division; DESNZ with NPSA; North Sea Transition Authority (NSTA)/Offshore Petroleum Regulator for Environment and Decommissioning (OPRED) (licensing, environment).	8.3, 14
Civil nuclear	Physical and cyber: Office for Nuclear Regulation (ONR) (Nuclear Industries Security Regulations 2003 (NISR)); Civil Nuclear Constabulary (CNC) (armed policing).	9
Rail	Cyber: Department for Transport (DfT) (NIS). Physical: DfT (National Railway Security Programme (NRSP)) and British Transport Police (BTP); Office of Rail and Road (ORR) (safety). NI: Department of Finance.	10.1
Road	Cyber: DfT (England and Wales (E&W)), Scottish Ministers, Department of Finance (NI). Physical: DfT/National Highways, Transport Scotland.	10.2
Aviation	Cyber: DfT + Civil Aviation Authority (CAA) (NIS; CAP 1753). Physical: CAA under the National Aviation Security Programme (NASP) set by DfT.	10.3
Space	CAA (Space Industry Act licences); UK Space Agency (UKSA)/Department for Science, Innovation and Technology (DSIT); Ofcom (spectrum).	10.3
Maritime and ports	Cyber: DfT (NIS). Physical: DfT Maritime Security (International Ship and Port Facility Security (ISPS)), Maritime and Coastguard Agency (MCA), Joint Maritime Security Centre (JMSC), Border Force.	10.4, 14
Telecoms	Cyber and physical: Ofcom (Telecommunications (Security) Act 2021 (TSA)); DSIT (codes, vendor directions).	11.1
Subsea cables	Ofcom (TSA), Ministry of Defence (MOD)/JMSC (protection); new statutory regime proposed (2026 white paper).	11.2, 14
Digital infrastructure (internet exchanges, DNS, domain registries)	Cyber: Ofcom (NIS).	11.3
Data centres	Proposed: DSIT (designation) + Ofcom (enforcement) under the Bill.	11.3
Digital services / managed	Cyber: Information Commissioner's Office (ICO) / Information Commission (NIS; Bill).	11.3

Network	Principal security regulators	See Section
service providers (MSPs)		
Water	Cyber: Drinking Water Inspectorate (DWI) (England, and for Welsh Ministers), Drinking Water Quality Regulator for Scotland (DWQR) (Scotland), Department of Finance (NI). Physical: Department for Environment, Food and Rural Affairs (Defra) Security and Emergency Measures Direction (SEMD) via DWI; Ofwat resilience.	12
Health	Cyber: Department of Health and Social Care (DHSC)/NHS England, Welsh and Scottish Ministers, Department of Finance (NI).	13
Finance	Cyber/operational resilience: Bank of England, Prudential Regulation Authority (PRA), Financial Conduct Authority (FCA) (incl. critical third parties).	13
Chemicals	HSE (Control of Major Accident Hazards Regulations 2015 (COMAH), incl. cyber to safety systems); NPSA/Counter Terrorism Policing; Home Office.	13
Emergency services, government, defence	LGD-led (Home Office, Cabinet Office, MOD) with NPSA/National Cyber Security Centre (NCSC); not NIS-designated.	13
Offshore assets (territorial sea, UK Continental Shelf (UKCS), Exclusive Economic Zone (EEZ))	NIS via sector CAs; HSE Energy Division; safety zones; ONR (nuclear transport); DfT/MCA/JMSC; Royal Navy; MMO and fisheries enforcement; marine licensing bodies.	14

1.2 Changes to watch (as at 18 September 2026)

- Cyber Security and Resilience Bill — Lords Report stage in progress; Royal Assent expected late 2026; secondary legislation and commencement to follow, bringing data centres, managed service providers (MSPs), load controllers and critical suppliers into regulation and introducing 24/72-hour incident reporting (Section 3.3 and 11.3).
- Downstream gas and electricity cyber regulation — Department for Energy Security and Net Zero (DESNZ) and Ofgem consultation (closed 22 May 2026) proposing to extend the Network and Information Systems Regulations to non-licensed participants and a Cyber Essentials-based baseline for all Ofgem licensees; government response awaited (Section 8.1).
- Undersea infrastructure protection — white paper on new subsea cable security legislation expected later in 2026, following the 29 May 2026 announcement and Joint Committee on the National Security Strategy reports (Sections 11.2 and 14).
- Martyn's Law — Terrorism (Protection of Premises) Act 2025: the Home Office published statutory guidance in April 2026, the Security Industry Authority (SIA) took on its regulatory duties on 15 June 2026 and its consultation on regulator guidance closed on 12 June 2026, with final guidance expected in autumn 2026; premises duties are expected to commence in spring 2027 (Sections 4 and 5).
- Water regulation reform — following the Independent Water Commission (2025), government proposals to consolidate Ofwat, Drinking Water Inspectorate (DWI) and parts of the Environment Agency into a single regulator for England and Wales; security functions (the Security and Emergency Measures Direction (SEMD) and the Network and Information Systems Regulations) will need re-allocation (Section 12).
- Rail reform — Great British Railways being established under the Railways Act 2025; Department for Transport (DfT) retains statutory security functions, but operator responsibilities will transfer (Section 10.1).

- Telecoms Security Code of Practice — updated code following the 2025–26 Department for Science, Innovation and Technology (DSIT) consultation; Ofcom compliance deadlines for Tier 1 and Tier 2 providers run to 2027–28 (Section 11.1).
- Food supply chain resilience — the National Audit Office report of 4 September 2026 found that the Department for Environment, Food and Rural Affairs (Defra) had not engaged sufficiently with industry, households and communities, identified cyber-attack as an increasingly likely risk to the food chain, and recommended a review of legal emergency powers; food remains outside the Network and Information Systems regime and the Bill, though the Bill's powers would allow it to be added by regulations (Section 5).
- Agricultural equipment security — the EU Cyber Resilience Act's reporting obligations apply to manufacturers selling into the EU from 11 September 2026 (full application 11 December 2027), while the UK's Product Security and Telecommunications Infrastructure Act 2022 still covers consumer connectable products only; the Agricultural Engineers Association is the industry's channel for pressing a secure-by-design standard for machinery and its data (Section 5.2).
- Waste crime — the Environmental Permitting (Waste Controlling or Transporting) Regulations 2026, laid in June 2026, will replace waste carrier, broker and dealer registration in England with permits after a twelve-month transition; digital waste tracking becomes mandatory for permitted sites in October 2026; the Waste Crime Action Plan (March 2026) funds Environment Agency enforcement for three years (Section 6.2).
- Fly-tipping and memorials — the Crime and Policing Act 2026 (Royal Assent 29 April 2026) provides for three to nine driving licence penalty points for fly-tipping with a vehicle, statutory enforcement guidance to councils and a new offence of climbing on specified memorials; commencement regulations are awaited (Sections 6.2 and 6.3).
- Freight crime — the Freight Crime Bill (recording and investigation of freight crime) awaits further Commons stages; the Home Office is piloting a freight crime flag on police recording systems in West Midlands Police ahead of national roll-out; the haulage trade associations continue to press for a specific offence and public funding for the industry-funded NaVCIS freight desk (Section 6.4).
- Rural crime — the National Police Chiefs' Council Rural and Wildlife Crime Strategy 2025–2028 (launched 25 November 2025) sets nine priorities; the Equipment Theft (Prevention) Act 2023 regulations (forensic marking and registration of new all-terrain vehicles and GPS units, without immobilisers) are still awaited; the Dogs (Protection of Livestock) (Amendment) Act 2025 came into force on 18 March 2026 and the Sentencing Council's hare coursing guideline on 1 June 2026; commencement of the Crime and Policing Act 2026 power to enter premises to recover electronically tracked stolen equipment is awaited (Section 7).
- Information Commission — Information Commissioner's Office (ICO) reconstituted under the Data (Use and Access) Act 2025, affecting the branding of the Network and Information Systems and managed service provider regulators (Section 4).

2. Purpose and scope

This document lists the UK bodies that regulate, oversee or set enforceable requirements for the physical security and cyber security of critical national infrastructure (CNI) networks, and of the rural land uses and crime regimes that surround them. It covers electricity, oil, gas, rail, road, communications, water, civil nuclear, aviation, maritime and ports, digital infrastructure (including data centres and subsea cables), health, finance, chemicals, space, defence, emergency services, food and government.

Geographic scope is the whole of the UK (England, Wales, Scotland and Northern Ireland), including offshore installations, pipelines, cables and wind farms within the UK territorial sea (12 nautical miles) and, where the relevant regime extends there, the UK Continental Shelf and Exclusive Economic Zone.

The guide is ordered for its readers rather than for the regulators. After the cross-cutting bodies in Sections 3 and 4, Section 5 deals with the farm-to-fork chain, Section 6 with the regimes that sit outside the critical national infrastructure framework but bear directly on rural estates (scrap metal dealing and metal theft, waste crime and fly-tipping, heritage crime affecting places of worship and heritage sites, and freight and cargo crime across the distribution network), and Section 7 with the land uses and rural crime regimes that the framework never reaches (construction sites and plant, remote energy sites, car boot sales and markets, forestry, inland fisheries, wildlife, livestock, equine, pet and firearms law, and the national bodies that set rural crime policy and count the cost). Sections 8 to 13 then set out the regulated networks sector by sector, and Section 14 deals specifically with the offshore dimension.

For each network the document identifies: the regulator or authority; whether its remit is physical security, cyber security, or both; the legal basis for its powers; and any pending changes. Where a body advises but does not regulate (for example the National Protective Security Authority and the National Cyber Security Centre), this is stated, because in several sectors physical security is delivered through Lead Government Department oversight and non-statutory advice rather than a licensed regulator.

3. How UK critical national infrastructure security regulation is organised

3.1 The 13 critical national infrastructure sectors and Lead Government Departments

The National Protective Security Authority (NPSA) defines UK critical national infrastructure as spanning 13 sectors: Chemicals, Civil Nuclear, Communications, Defence, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport and Water. Each sector has one or more Lead Government Departments (LGDs) responsible for the sector and for ensuring protective security is in place for critical assets. Lead Government Departments identify and classify which infrastructure is genuinely 'critical' against the official UK definition (assets whose loss or compromise would have a major detrimental impact on essential services, national security or the economy).

3.2 The three National Technical Authorities

Three bodies provide the UK's authoritative protective security advice and work together: the National Cyber Security Centre (NCSC), part of GCHQ, for cyber security; the National Protective Security Authority, part of MI5 and formerly the Centre for the Protection of National Infrastructure, for physical and personnel security, countering terrorism and hostile state activity; and UK NACE (the National Authority for Counter-Eavesdropping) for technical security. None of the three is a regulator with enforcement powers; their frameworks (for example the National Cyber Security Centre's Cyber Assessment Framework (CAF)) are adopted by the sector regulators below as the basis for compliance assessment.

3.3 The cyber security regulatory model: Network and Information Systems Regulations 2018

Statutory cyber security regulation of critical national infrastructure operators rests principally on the Network and Information Systems Regulations 2018 (SI 2018/506), which implemented the EU Network and Information Systems Directive and were retained after EU exit. The Regulations designate 'Operators of Essential Services' (OES) in energy, transport, health, drinking water and digital infrastructure, and 'Relevant Digital Service Providers' (RDSPs). Each sector has a 'Competent Authority' (CA), listed in Schedule 1, responsible for designating operators, issuing guidance, monitoring compliance, receiving incident reports and enforcing (penalties up to £17 million). The Department for Science, Innovation and Technology (DSIT) owns the Network and Information Systems policy framework; the National Cyber Security Centre is the Single Point of Contact and technical authority; and the Information Commissioner's Office (ICO) regulates digital service providers.

Status: Cyber Security and Resilience (Network and Information Systems) Bill

The Bill was introduced in the House of Commons on 12 November 2025, completed its Commons stages in June 2026, had its Lords second reading in July 2026 and Lords Grand Committee stage from 1 September 2026. As at 16 September 2026 it is at Lords Report stage (current print: HL Bill 49, as amended in Grand Committee, 7 September 2026). Royal Assent is widely expected in late 2026, with most substantive obligations commenced through secondary legislation thereafter.

The Bill amends (rather than replaces) the Network and Information Systems Regulations. It brings into scope data centres (colocation above 1 MW rated IT load; enterprise data centres of 10 MW or more), managed service providers, large load controllers and designated critical suppliers; introduces a two-stage incident reporting duty (initial notification within 24 hours, full report within 72 hours, to the regulator and

National Cyber Security Centre); strengthens regulators' information-gathering, cost-recovery and enforcement powers; and gives the Secretary of State power to update the regime by regulations. Where this document names a regulator's role as 'proposed' or 'expected', that role depends on the Bill and its secondary legislation.

3.4 The physical security model

There is no single statutory physical security regime for critical national infrastructure equivalent to the Network and Information Systems Regulations. Physical protective security is instead delivered through: sector-specific statutory regimes where they exist (civil nuclear, aviation, maritime and ports, rail, and the Channel Tunnel); Lead Government Department oversight of critical national infrastructure assets with National Protective Security Authority advice and the National Protective Security Authority and National Cyber Security Centre assurance frameworks; emergency powers held by Secretaries of State (for example directions under the Electricity Act 1989 and Energy Act 1976); Counter Terrorism Policing (including Counter Terrorism Security Advisers and National Counter Terrorism Security Office (NaCTSO)) and, from spring 2027, the Security Industry Authority as regulator of the Terrorism (Protection of Premises) Act 2025 ('Martyn's Law'). Health, safety and major-accident regulation by the Health and Safety Executive and the Office for Nuclear Regulation also imposes enforceable requirements on the integrity and protection of hazardous infrastructure, which overlap substantially with security.

4. Cross-cutting national bodies

The following bodies have a role across all or most critical national infrastructure sectors. They are listed before the sector tables because they are referenced repeatedly.

Body	Role in critical national infrastructure (CNI) security
National Cyber Security Centre (NCSC)	Part of GCHQ. UK national technical authority for cyber security. Owns the Cyber Assessment Framework (CAF), Cyber Essentials and sector cyber guidance; Network and Information Systems (NIS) Single Point of Contact and incident-response lead; will receive significant-incident reports alongside sector regulators under the Bill. Advisory, not a regulator.
National Protective Security Authority (NPSA)	Part of MI5 (formerly Centre for the Protection of National Infrastructure (CPNI)). National technical authority for physical and personnel security; advises CNI operators, Lead Government Departments (LGDs) and regulators on protective security against terrorism and state threats; maintains the CNI sector list; publishes standards (e.g. Catalogue of Security Equipment, Operational Requirements, Trusted Research). Advisory, not a regulator.
UK NACE	National Authority for Counter-Eavesdropping (Foreign, Commonwealth and Development Office). Technical security (technical surveillance countermeasures (TSCM), radio frequency (RF), acoustic) advice for CNI and government. Advisory.
Department for Science, Innovation and Technology (DSIT)	Policy owner for the NIS Regulations and the Cyber Security and Resilience Bill; Lead Government Department (LGD) for the Communications and Space sectors (with the UK Space Agency); sponsor of the Telecommunications (Security) Act 2021; policy lead on data centres (designated CNI in September 2024) and on the proposed subsea cable security legislation announced 29 May 2026.
Cabinet Office	National Security Secretariat and Resilience Directorate: the National Security Risk Assessment, Civil Contingencies Act 2004 framework, COBR, the UK Government Resilience Framework and the CNI Knowledge Base; GovAssure (cyber assurance of government systems, using the CAF); home of the Investment Security Unit administering the National Security and Investment Act 2021 (mandatory notification for acquisitions in 17 sensitive sectors, including energy, transport, communications, data infrastructure and civil nuclear).
Home Office	LGD for Emergency Services and for counter-terrorism policy (CONTEST); sponsors Counter Terrorism Policing, the National Counter Terrorism Security Office (NaCTSO) and the Counter Terrorism Security Adviser (CTSA) network which delivers protective security advice at sites; sponsor of Martyn's Law and of the Security Industry Authority; co-leads the Joint Maritime Security Centre.
Security Industry Authority (SIA)	Statutory regulator of the private security industry (Private Security Industry Act 2001: licensing of security operatives and the Approved Contractor Scheme). Designated regulator for the Terrorism (Protection of Premises) Act 2025 ('Martyn's Law'). The Act received Royal Assent on 3 April 2025; the SIA's duties to prepare regulatory guidance and define 'qualifying worldwide revenue' commenced on 15 June 2026 (Commencement No. 2 Regulations 2026); the premises duties are expected to commence in spring 2027. Statutory guidance (Home Office, April 2026) sets the tiers: standard tier where 200 to 799 individuals, including staff, may reasonably be expected to be present at the same time from time to time; enhanced tier where the figure is 800 or more. Qualifying uses in Schedule 1 include shops, shopping centres, fuel stations, food and drink premises, transport hubs, stadia and public buildings, many of them within CNI estates.
Information Commissioner's Office (ICO) / Information Commission	NIS Competent Authority for relevant digital service providers (cloud, online marketplaces, search) and, under the Bill, expected regulator of managed service providers. Regulator of UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018, including personal data breach reporting (72 hours). Being reconstituted as the Information Commission under the Data (Use and Access) Act 2025.
Counter Terrorism Policing / NaCTSO / Counter Terrorism Security Advisers (CTSAs)	Police-led protective security advice and site assessments for CNI and crowded places; ProtectUK platform; enforcement of terrorism offences. Not a licensing regulator, but a primary physical-security interlocutor for operators.

Body	Role in critical national infrastructure (CNI) security
Office for Product Safety and Standards (OPSS)	Enforces Part 1 of the Product Security and Telecommunications Infrastructure Act 2022 (security requirements for consumer connectable products), relevant to IoT devices deployed in infrastructure estates. Business and industrial connectable products, including agricultural machinery and its telematics, are outside its scope (Section 5.2).
Ministry of Defence / Royal Navy / Joint Maritime Security Centre (JMSC)	Protection of undersea infrastructure and maritime domain awareness (e.g. Royal Fleet Auxiliary (RFA) Proteus, Atlantic Bastion); JMSC is the multi-agency maritime security coordination centre (Home Office, Ministry of Defence (MOD), Department for Transport (DfT), Border Force, Maritime and Coastguard Agency (MCA), police). Defence CNI is regulated internally by MOD (e.g. Defence Nuclear Safety Regulator, MOD Police).
Health and Safety Executive (HSE)	Regulator of major-hazard and process safety onshore and offshore: Control of Major Accident Hazards Regulations 2015 (COMAH) (chemicals, fuel storage), Pipelines Safety Regulations 1996, Offshore Installations (Offshore Safety Directive) (Safety Case) Regulations 2015, gas safety, and rail (via Office of Rail and Road (ORR)). HSE requires operators to address cyber-related causes of major accidents in safety cases and Operational Guidance (OG86) sets its inspection approach to industrial control system cyber security.

5. Food, farming and fisheries: the farm-to-fork chain

Food is one of the 13 critical national infrastructure sectors, with Defra as Lead Government Department, but it is the sector with the thinnest statutory security architecture.

Neither farming, fisheries, food manufacturing nor food distribution is designated under the Network and Information Systems Regulations 2018; the Cyber Security and Resilience Bill does not add them (although it gives the Secretary of State a power to add sectors by regulations); and agriculture is not among the 17 mandatory-notification sectors under the National Security and Investment Act 2021.

Physical and cyber security across the chain is therefore delivered by Lead Government Department oversight, non-statutory advice from the National Cyber Security Centre, the National Protective Security Authority, the National Farmers' Union (NFU) and Counter Terrorism Policing, and a patchwork of bodies whose primary remit is safety, biosecurity, licensing or economic regulation rather than security.

Defra's Food Supply Chain Resilience team leads on resilience planning, supported by the statutory UK Food Security Report (Agriculture Act 2020 s.19; latest edition 11 December 2024), the annual Food Security Index, the Food Resilience Industry Forum (activated during disruption) and the government's Food Strategy for England (July 2025). The National Audit Office report of 4 September 2026, 'Resilience of the food supply chain to disruptions', found that Defra has not engaged sufficiently with industry, households and communities since the pandemic, identified cyber-attack as an increasingly likely risk alongside extreme weather and animal or plant disease, and recommended that Defra review its legal emergency powers and test response plans with industry and local government.

5.1 Regulators and authorities across the chain

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
Primary agricultural production (arable, livestock, horticulture, dairy, farm estates)	Department for Environment, Food and Rural Affairs (Defra) — Lead Government Department (LGD) (England); Welsh Government; Scottish Government; Department of Agriculture, Environment and Rural Affairs (DAERA) (NI); Rural Payments Agency; police forces and the National Rural Crime Unit; National Cyber Security Centre (NCSC) and National Protective Security Authority (NPSA) (advice)	No statutory security regulator. Cyber: NCSC/National Farmers' Union (NFU) 'Cyber security for farmers' guidance (2023) and NCSC small-business guidance; nothing enforceable. Physical: police rural crime teams, the National Rural Crime Unit (est. 2023) and National Police Chiefs' Council (NPCC) Rural and Wildlife Crime lead; NPSA/Counter Terrorism Security Adviser (CTSA) advice for larger estates and agri-businesses.	Agriculture Act 2020 (s.19 UK Food Security Report); Agriculture (Wales) Act 2023; Agriculture and Rural Communities (Scotland) Act 2024. Equipment Theft (Prevention) Act 2023 (forensic marking and immobilisers on all-terrain vehicles (ATVs) and equipment; commencement regulations pending). Civil Contingencies Act 2004 (farmers are not Category 1 or 2 responders).
Agricultural inputs: fertiliser, explosives precursors, pesticides, veterinary medicines,	Health and Safety Executive (HSE) (ammonium nitrate, pesticides via the Chemicals Regulation Division); Home Office (explosives precursors and poisons licensing; National Counter Terrorism Security Office (NaCTSO) fertiliser security	Physical: statutory controls on the storage, supply and reporting of high-nitrogen ammonium nitrate and regulated explosives precursors, with counter-terrorism guidance on secure storage; pesticide and veterinary medicine supply controls. Fuel and water supply security follow the energy and water regimes (Sections 8 and 12).	Ammonium Nitrate Materials (High Nitrogen Content) Safety Regulations 2003; Poisons Act 1972 and Control of Explosives Precursors and Poisons Regulations

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
feed, fuel and water	guidance with the Agricultural Industries Confederation); Veterinary Medicines Directorate; Food Standards Agency (FSA) and local authorities (feed); Environment Agency / Natural Resources Wales (NRW) / Scottish Environment Protection Agency (SEPA) (abstraction)		2023; Plant Protection Products (Sustainable Use) Regulations 2012; Veterinary Medicines Regulations 2013; Water Resources Act 1991.
Agricultural machinery, robotics, automation and connected equipment (tractor and combine telematics, autonomous field robots, robotic milking and feeding, precision sprayers, drones, sensors, gauges and data loggers)	No security regulator. Office for Product Safety and Standards (consumer connectable products only); HSE (machinery safety at work); Department for Transport (DfT) / Vehicle Certification Agency (road-going and automated vehicles); Agricultural Engineers Association (AEA) (trade body; runs the CESAR marking scheme; advisory); NCSC and NPSA (advice)	Physical: equipment marking and immobilisers (CESAR scheme; Equipment Theft (Prevention) Act 2023 regulations pending); police rural crime teams. Cyber: no statutory requirement for business or industrial agricultural equipment; the Product Security and Telecommunications Infrastructure Act 2022 covers consumer products only; manufacturers selling into the EU must meet the EU Cyber Resilience Act (vulnerability and incident reporting from 11 September 2026, full application from 11 December 2027). See Section 5.2.	Product Security and Telecommunications Infrastructure Act 2022 Part 1 and the Product Security Regulations 2023 (in force 29 April 2024; consumer connectable products); Supply of Machinery (Safety) Regulations 2008; Equipment Theft (Prevention) Act 2023; Automated Vehicles Act 2024 (road use); Regulation (EU) 2024/2847 (Cyber Resilience Act) for EU market access.
Animal and plant health biosecurity (disease surveillance, outbreak control, laboratories)	Animal and Plant Health Agency (APHA, Defra executive agency acting for England, Wales and Scotland); Defra Chief Veterinary Officer; DAERA (NI); Science and Advice for Scottish Agriculture (SASA) and Scottish Government; Forestry Commission (tree health); Pirbright Institute and APHA Weybridge (reference laboratories); HSE (specified animal pathogens)	Physical and biosecurity: statutory notifiable-disease regime, movement controls, culling and licensing; secure laboratory containment for animal pathogens is licensed jointly by APHA and HSE. Cyber: livestock and plant traceability systems (e.g. Livestock Information Service) are Defra/APHA systems assured under government cyber standards (GovAssure).	Animal Health Act 1981; Plant Health Act 1967; Plant Health (Official Controls) Regulations 2019 (retained EU 2016/2031 and 2017/625); Specified Animal Pathogens Order 2008; Animal Welfare Act 2006.
Border biosecurity and food imports (ports, airports, border control posts)	Defra (sanitary and phytosanitary (SPS) policy); Border Force (Home Office); port health authorities (local authorities, e.g. Dover Port Health Authority); APHA and inland border control posts; FSA and Food Standards Scotland (FSS); DAERA (NI, under the Windsor Framework)	Physical: checks on commercial imports at border control posts under the Border Target Operating Model (introduced April 2023, phased in 2024) and enforcement of personal import rules by Border Force; the Environment, Food and Rural Affairs (EFRA) Committee report 'Biosecurity at the border' (8 September 2025) found significant enforcement gaps and recommended a ministerial taskforce, stop-search-seize powers for port health authorities and expanded Dover coverage.	Official Controls (Plant Health and Genetically Modified Organisms) Regulations 2019; Trade in Animals and Related Products Regulations 2011; Customs and Excise Management Act 1979; Border Target Operating Model

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
			(Defra/Cabinet Office).
Fisheries, aquaculture and fishing ports	Marine Management Organisation (England); Marine Directorate (Scotland); Welsh Government; DAERA (NI); Inshore Fisheries and Conservation Authorities; Royal Navy Overseas Patrol Squadron (fishery protection, under agreement with the Marine Management Organisation (MMO)); Maritime and Coastguard Agency (MCA) (fishing vessel safety); Centre for Environment, Fisheries and Aquaculture Science (Cefas) Fish Health Inspectorate (aquaculture); harbour authorities	Physical: licensing, monitoring (vessel monitoring systems, electronic logbooks, remote electronic monitoring) and at-sea enforcement of the UK fisheries regime out to the 200 nm limit; fishing vessel safety codes; International Ship and Port Facility Security (ISPS) security applies only where a fishing port also handles ISPS-regulated traffic (Section 10.4). Cyber: no regulator; vessel monitoring and catch systems are MMO/devolved-administration government systems.	Fisheries Act 2020 (Joint Fisheries Statement 2022); Sea Fish (Conservation) Act 1967; Merchant Shipping Act 1995 and Fishing Vessels (Safety) codes; Aquatic Animal Health (England and Wales) Regulations 2009; Marine and Coastal Access Act 2009.
Food and drink processing and manufacturing (abattoirs, dairies, mills, bakeries, breweries, processors)	Food Standards Agency (England, Wales, NI) and Food Standards Scotland; local authority environmental health and trading standards; FSA National Food Crime Unit (NFCU); HSE (major hazards, e.g. ammonia refrigeration); Information Commissioner's Office (ICO) (personal data)	Physical: food safety and hygiene regulation, FSA official controls in approved establishments (meat, dairy), and the National Food Crime Unit's investigation of deliberate contamination, adulteration and fraud (the NFCU was granted Police and Criminal Evidence Act 1984 (PACE) search-warrant powers from 1 May 2025). Cyber: no regulator; incidents affecting personal data reportable to ICO; NCSC advice only. Food manufacturers are excluded from the Network and Information Systems (NIS) regime and the Bill.	Food Safety Act 1990; retained Regulation (EC) 178/2002 (General Food Law), 852/2004 and 853/2004; Official Controls Regulations 2017/625 as retained; Police and Criminal Evidence Act 1984 (NFCU powers); Control of Major Accident Hazards Regulations 2015 (COMAH).
Cold chain, storage, wholesale and logistics (chilled and frozen warehousing, haulage, distribution centres)	Defra (resilience and Food Resilience Industry Forum); DfT — Traffic Commissioners and Driver and Vehicle Standards Agency (DVSA) (haulage operator licensing and roadworthiness); HSE (ammonia and pressure systems); Ofgem/Department for Energy Security and Net Zero (DESNZ) (energy dependence); Groceries Code Adjudicator (economic)	Physical: no security regulator; voluntary standards (e.g. Transported Asset Protection Association (TAPA) facility, trucking and parking security, Brand Reputation Compliance Global Standards (BRCGS) Storage and Distribution) and insurer requirements govern site and cargo security; DfT's road, port and rail regimes (Section 10) cover the transport infrastructure itself. Theft of goods in transit is recorded by the police as theft from a vehicle and collated only by the industry-funded National Vehicle Crime Intelligence Service freight desk (Section 6.4). Cyber: none; sector highly dependent on the energy, telecoms and data-centre regimes in Sections 8 and 11.	Goods Vehicles (Licensing of Operators) Act 1995; Food Hygiene (England) Regulations 2013 (temperature control); Groceries Code Adjudicator Act 2013.
Retail and food service (supermarkets, distribution networks, hospitality)	Local authorities and FSA/FSS; Security Industry Authority (SIA) (Martyn's Law, premises duties expected from spring 2027); ICO; police and Counter	Physical: Martyn's Law will apply to shops, supermarkets, shopping centres, fuel stations and food and drink premises where 200 or more individuals (including staff) may reasonably be expected to be present at the same time; the test is expected attendance at	Terrorism (Protection of Premises) Act 2025; Data Protection Act 2018; Food Safety Act 1990.

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
	Terrorism Policing (crowded places)	the busiest times, not fire capacity or floor area, and a store that exceeds 200 during seasonal peaks 'from time to time' is caught. Each store is assessed separately; a shopping centre operator aggregates the footfall of all units for the centre's own tier. Standard tier (200 to 799): notify the SIA and have evacuation, invacuation, lockdown and communication procedures. Enhanced tier (800 or more): additionally document risk-assessed protective measures (monitoring, movement control, physical security, information security) and submit them to the SIA. NaCTSO crowded places guidance; local policing. Cyber: none specific; UK General Data Protection Regulation (GDPR) and Payment Card Industry Data Security Standard (PCI-DSS) obligations; NCSC retail guidance. Major retailer ransomware incidents in 2025 demonstrated the concentration risk in retail supply chains.	
Cross-cutting: food supply chain resilience and emergency powers	Defra Food Supply Chain Resilience team; Cabinet Office (National Security Risk Assessment, resilience framework); Food Resilience Industry Forum; Food and Drink Sector Council; devolved administrations; local resilience forums	Planning and coordination rather than regulation: UK Food Security Report (every three years), Food Security Index (annual), scenario exercising, and emergency powers under the Civil Contingencies Act and retained food-supply legislation. The National Audit Office (NAO) (September 2026) recommended Defra review whether existing legal powers are adequate for a catastrophic food supply disruption.	Agriculture Act 2020 s.19; Civil Contingencies Act 2004 Part 2 (emergency regulations); Emergency Powers legacy provisions; Food Strategy for England (July 2025); UK Government Resilience Framework (2022, updated 2025).

5.2 Agricultural technology, connected machinery and the Agricultural Engineers Association

Farming is now an operational technology environment. Tractors and combines run on satellite guidance and report to the manufacturer's telematics cloud; milking, feeding, ventilation and irrigation are automated; sprayers and spreaders are rate-controlled from prescription maps; drones and autonomous field robots are moving from trials into commercial use; and grain stores, cold stores, slurry systems, fuel tanks and livestock buildings are watched by sensors, gauges and data loggers that feed farm-management and dealer platforms.

Every one of these is a networked computer with firmware, a remote-access path and, usually, a cloud account controlled by the manufacturer or the dealer. A compromise can stop machinery mid-season, disable ventilation or milking, corrupt the spray, medicine and traceability records that the food chain relies on, or expose commercially sensitive data on land, inputs and yields. Yet nothing in Section 5.1 obliges anyone to secure this equipment or to report an attack on it.

The thinnest part of the picture is the obligation on manufacturers. The Product Security and Telecommunications Infrastructure Act 2022, enforced by the Office for Product Safety and Standards since 29 April 2024, requires unique passwords, a vulnerability disclosure policy and a stated security-update period, but only for consumer connectable products. It catches a smart doorbell on the

farmhouse and not the telematics unit on a combine, the controller on a robotic milking installation or the gateway on a grain-store monitoring system, all of which are business products outside its scope.

The European Union has gone further with the Cyber Resilience Act, which requires manufacturers placing any product with digital elements on the EU market to report actively exploited vulnerabilities and severe incidents from 11 September 2026 and to meet full secure-by-design and vulnerability-handling requirements from 11 December 2027. UK manufacturers who export will therefore be building to that standard; UK farmers buying for the UK market have no equivalent statutory assurance. The Cyber Security and Resilience Bill's power to add sectors by regulations could in principle close the gap, but neither it nor the Government's product security regime is currently directed at agricultural equipment.

The Agricultural Engineers Association (AEA), founded in 1875, is the trade body for manufacturers and importers of agricultural machinery and outdoor power equipment. It represents the sector to Government, Parliament and the media, publishes the industry's trade statistics, administers the CESAR equipment-marking and registration scheme (Construction and Agricultural Equipment Security and Registration) and the National Sprayer and Spreader Testing Scheme, and is the UK member of CEMA, the European agricultural machinery association through which manufacturers engage with European standards and the Cyber Resilience Act. It is not a regulator and has no enforcement powers.

It is, however, the only body with a standing channel to Defra, the Department for Transport and the Department for Science, Innovation and Technology, membership across the manufacturer base and scheme infrastructure already in place, which makes it the natural advocate for a secure-by-design expectation in agricultural machinery: secure default configuration, authenticated and logged dealer remote access, signed firmware with a published support period, a vulnerability disclosure and patching commitment, and clear rules on who owns, and who may access, the data generated by machines and by the instruments and gauges fitted to them.

That data is often the most sensitive asset on the machine and the least protected when the equipment is sold, hired, serviced, exported or stolen. The Agricultural Engineers Association is equally well placed to carry these expectations into the schemes it runs, so that CESAR registration or sprayer testing could in time include a check that a connected machine has been secured and that its stored data has been handled correctly.

Until manufacturers are brought within a product security regime, the assurance available to farmers and estates is contractual and practical rather than statutory: asking manufacturers and dealers for their vulnerability disclosure policy, support period and remote-access arrangements before purchase; keeping machine, sensor and building-control networks separate from office systems; controlling and logging dealer and contractor remote access; wiping or transferring stored data when equipment changes hands; and following the National Cyber Security Centre and National Farmers' Union guidance for farmers. Rural SafeGuard's view is that this is a gap in the national framework rather than a matter for individual farms, and that the Agricultural Engineers Association, the farming unions and insurers should press it jointly.

5.3 Where the gaps are

Four features of the sector matter for anyone assessing risk.

- First, there is no cyber regulator and no mandatory incident reporting anywhere in the chain, so a ransomware attack on a processor, a cold-store operator or a farm-management platform is not reportable to any authority unless personal data is involved (Information Commissioner's Office) or it becomes a food safety incident (Food Standards Agency).
- Second, physical security is enforced only where it overlaps with another regime: counter-terrorism controls on fertiliser and precursors, biosecurity controls on animals and plants, the

International Ship and Port Facility Security (ISPS) Code at the largest ports, and, from spring 2027, Martyn's Law at retail and food premises expecting 200 or more people at a time. Everything else rests on police advice, insurer conditions and voluntary standards.

- Third, the chain's resilience is inherited from the regulated networks it depends on: electricity for cold storage, diesel for machinery and haulage, telecoms and data centres for just-in-time ordering, water for processing and irrigation, and ports and roads for imports and distribution, all of which are covered in Sections 8 to 12 and 14.
- Fourth, the machinery, robotics and sensors on which the chain increasingly runs sit outside product security regulation altogether, because the Product Security and Telecommunications Infrastructure Act 2022 reaches consumer products only (Section 5.2).

6. Scrap metal, waste, heritage and freight crime

The four regimes in this section sit outside the critical national infrastructure framework, but they matter to anyone responsible for a rural estate, a church, a heritage site or a distribution operation, and three of them feed directly into the security of the networks and supply chains described in Sections 8 to 14.

Metal stolen from railway signalling cable, telecommunications cable, substation earthing, church roofs and war memorials is turned into money through the scrap metal trade, so the licensing of scrap metal dealers is in practice a control on the end market for infrastructure and heritage theft.

Waste crime and fly-tipping fall disproportionately on farmland and private access roads, where the landowner rather than the public purse carries the clearance cost.

Heritage crime is concentrated on the most exposed assets in the countryside: parish churches, chapels, monuments and the fabric of historic estates.

Freight crime, the theft of goods in transit and from the lorry parks, laybys and distribution centres that serve the food chain, is the least visible of the four because the police record it as ordinary theft from a vehicle.

Each regime has a different model. Scrap metal dealing is licensed by local authorities and policed by the police, with the Home Office as policy owner. Waste is regulated by the four environmental regulators (the Environment Agency in England, Natural Resources Wales, the Scottish Environment Protection Agency and the Northern Ireland Environment Agency) with local authorities enforcing fly-tipping at street level.

Heritage protection rests on planning and consent law administered by local planning authorities and the national heritage bodies, with the police and the Crown Prosecution Service prosecuting the underlying offences of theft and criminal damage.

Freight crime has no lead body at all: the only statutory security regimes for cargo are the aviation and maritime ones described in Section 10, and road freight, which carries most of the country's food, relies on an industry-funded police intelligence unit and voluntary standards.

None of the four has a dedicated security regulator; as in the food chain, protection is delivered through licensing conditions, partnerships and police enforcement rather than through statutory security duties on owners.

6.1 Scrap metal dealers and metal theft

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
Scrap metal dealers and mobile collectors (England and Wales)	Local authorities (licensing authority: site licences and collector's licences, three-year term); police (constables and local authority officers have powers of entry and inspection); Home Office (policy owner; Post Implementation Review, January 2022); HM Revenue and Customs (tax check on renewals since 4 April 2022); Environment Agency /	Physical: the Scrap Metal Dealers Act 2013 makes it an offence to carry on business as a scrap metal dealer without a licence, bans payment in cash (s.12), requires dealers to verify the seller's name and address (s.11) and to keep records of every item received and disposed of (ss.13–14), and allows closure notices and orders against unlicensed sites. Licences may be refused or revoked where the applicant is not a suitable person, taking account of relevant convictions. The Home Office review in 2022 concluded the Act should be retained; Historic England and the National Infrastructure Crime Reduction Partnership have pressed for more consistent local	Scrap Metal Dealers Act 2013; Scrap Metal Dealers Act 2013 (Prescribed Relevant Offences and Relevant Enactments) Regulations 2013; Finance Act 2021 s.125 and Schedule 33 (tax conditionality for licence renewals); Environmental Permitting (England and Wales)

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
	Natural Resources Wales (environmental permit for the site)	authority and police enforcement, particularly of mobile collectors. Cyber: none.	Regulations 2016 (site permits).
Metal dealers (Scotland)	Local authorities (licensing under the Civic Government (Scotland) Act 1982); Police Scotland; Scottish Government; HM Revenue and Customs (tax check on renewals since 2 October 2023)	Physical: metal dealers and itinerant metal dealers must hold a local authority licence; payment must be by non-transferable cheque or electronic transfer (cash ban in force since 1 September 2016); records of acquisition and disposal must be kept for three years; a register of licensed dealers is maintained. Cyber: none.	Civic Government (Scotland) Act 1982 as amended by the Air Weapons and Licensing (Scotland) Act 2015 Part 3 (metal dealers).
Metal recycling (Northern Ireland)	Northern Ireland Environment Agency (waste management licensing and carrier registration; Department of Agriculture, Environment and Rural Affairs); Police Service of Northern Ireland; HM Revenue and Customs	Physical: there is no Northern Ireland equivalent of the Scrap Metal Dealers Act 2013. A Scrap Metal Dealers Bill introduced in the Assembly in 2015 lapsed at the end of the mandate. Metal recycling sites require a waste management licence and collectors must be registered waste carriers, but there is no statutory cash ban or seller-identification duty; the metal-theft controls are the ordinary criminal law and waste licensing conditions. Cyber: none.	Waste and Contaminated Land (Northern Ireland) Order 1997; Controlled Waste (Registration of Carriers and Seizure of Vehicles) Regulations (Northern Ireland) 1999; Finance Act 2021 (tax conditionality).
Metal theft from infrastructure and heritage assets (railway cable, telecommunications cable, substations, church roofs, war memorials, farm and estate metalwork)	Police forces; British Transport Police (rail; hosts the National Infrastructure Crime Reduction Partnership with Network Rail, Openreach, the energy networks, the Church of England and Historic England); Opal (national intelligence unit for serious organised acquisitive crime); National Police Chiefs' Council lead for metal theft; Home Office; Crown Prosecution Service	Physical: prosecution of theft, handling and criminal damage; the Sentencing Council theft guideline treats damage to heritage assets and disruption to infrastructure or public services as aggravating harm. The Church of England and Ecclesiastical Insurance require roof alarms and forensic marking as insurance conditions, and Historic England advises on replacing stolen lead with less attractive materials. The National Infrastructure Crime Reduction Partnership coordinates intelligence and 'days of action' at scrap yards with local authorities. Cyber: none; cable theft is nonetheless a recognised cause of rail signalling and telecommunications outages.	Theft Act 1968; Criminal Damage Act 1971; Sentencing Council, Theft Offences: Definitive Guideline (2016); Police, Crime, Sentencing and Courts Act 2022 s.50 (criminal damage to memorials triable either way regardless of value, maximum ten years); Crime and Policing Act 2026 s.161 (climbing on specified memorials).

6.2 Waste management, waste crime and fly-tipping

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
Waste operators, sites, carriers, brokers and dealers (England)	Environment Agency — permitting and enforcement; Joint Unit for Waste Crime (Environment Agency-led with police, the National Crime Agency, HM Revenue and Customs, Natural	Physical: environmental permits and registered exemptions for waste sites; the duty of care on every holder of waste (Environmental Protection Act 1990 s.34); waste carrier, broker and dealer registration, which the Environmental Permitting (Waste Controlling or Transporting) Regulations 2026 will replace with a permitting regime requiring technical competence and background checks, with a twelve-month transition after approval and	Environmental Protection Act 1990 ss.33, 33A–33C, 34 and 59; Environmental Permitting (England and Wales) Regulations 2016; Control of Pollution

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
	Resources Wales, the Scottish Environment Protection Agency and the Northern Ireland Environment Agency; expanded to 20 staff in 2026); Department for Environment, Food and Rural Affairs (Defra) — policy; HM Revenue and Customs (landfill tax); National Crime Agency	offences carrying up to five years' imprisonment; three waste exemptions removed and seven tightened; mandatory digital waste tracking for permitted sites from October 2026. The Waste Crime Action Plan (20 March 2026) adds £45 million over three years for Environment Agency enforcement, an Operational Waste Intelligence and Analysis Unit using satellite, drone and financial data, and a consultation on conditional cautions with unpaid work. In 2025–26 the Joint Unit for Waste Crime led 23 operations, supported 38 more and delivered 111 disruptions. Cyber: the digital waste tracking service is a Defra and Environment Agency system; there is no cyber requirement on operators.	(Amendment) Act 1989 and Waste (England and Wales) Regulations 2011 (carrier, broker and dealer registration, pending replacement); Environment Act 2021; Finance Act 1996 Part III (landfill tax).
Waste regulation (Wales, Scotland and Northern Ireland)	Natural Resources Wales and Welsh Government; Scottish Environment Protection Agency and Scottish Government; Northern Ireland Environment Agency Environmental Crime Unit (established 2008) within the Department of Agriculture, Environment and Rural Affairs	Physical: the same permitting, duty of care and carrier registration model applies in each nation, with the 2026 carrier, broker and dealer reforms currently England-only. Scotland raised the fly-tipping fixed penalty to £500 on 1 January 2024 and the Circular Economy (Scotland) Act 2024 strengthens fly-tipping offences and cost recovery. The Northern Ireland Audit Office (10 July 2025) estimated at least 300,000 tonnes of waste is dumped illegally each year, with the Mobuoy site alone holding around 1.6 million tonnes, and found the Environmental Crime Unit carrying 22 vacancies. Cyber: none.	Environmental Protection Act 1990 (Wales and Scotland); Circular Economy (Scotland) Act 2024; Fly-tipping (Fixed Penalty) (Scotland) Order 2023; Waste and Contaminated Land (Northern Ireland) Order 1997; Waste Management Licensing Regulations (Northern Ireland) 2003.
Fly-tipping, including on farmland and private land (England and Wales)	Local authorities (primary enforcement body for fly-tipping; fixed penalty notices, prosecutions, vehicle seizure); Environment Agency / Natural Resources Wales (large-scale, hazardous or organised dumping); police (vehicle offences and, from commencement, penalty points); magistrates' and Crown courts; National Fly-Tipping Prevention Group (Defra-chaired, with the National Farmers' Union, the Country Land and Business Association and local government); National Rural Crime Unit	Physical: fly-tipping is an offence under Environmental Protection Act 1990 s.33 (unlimited fine and up to five years' imprisonment on indictment). Local authorities may issue fixed penalties of up to £1,000 for fly-tipping and up to £600 for a householder who passes waste to an unlicensed carrier, may seize and dispose of vehicles used in fly-tipping, and may serve a section 59 notice requiring the occupier of land to remove waste, which the occupier can resist only by showing they neither deposited nor knowingly permitted it. There is no public duty to clear waste dumped on private land, so farmers and estates bear the removal and lawful disposal cost. The Crime and Policing Act 2026 empowers courts to endorse three to nine penalty points on the licence of a driver convicted of fly-tipping with a vehicle (s.10) and allows Defra to issue statutory enforcement guidance to councils, including on vehicle seizure (s.9). England recorded 1.26 million fly-tipping incidents in 2024–25, up 9 per cent, with 572,000 enforcement actions, 69,000 fixed penalties and only 1,250 court fines totalling £673,000. Cyber: none.	Environmental Protection Act 1990 ss.33, 33A–33C, 34(2A), 59; Unauthorised Deposit of Waste (Fixed Penalties) Regulations 2016 as amended; Environmental Offences (Fixed Penalties) (Miscellaneous Provisions) Regulations 2017; Control of Waste (Dealing with Seized Property) (England and Wales) Regulations 2015; Crime and Policing Act 2026 ss.9–10 (Royal Assent 29 April 2026; commencement by regulations).

6.3 Heritage crime: places of worship and national heritage sites

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
Listed buildings, scheduled monuments and registered parks, battlefields and wrecks (England)	Historic England (statutory adviser; Heritage Crime Programme since 2011; convenes the Alliance to Reduce Crime against Heritage (ARCH) and the Heritage Watch network); local planning authorities (listed building and scheduled monument enforcement); Department for Culture, Media and Sport (Lead Government Department; designation); police forces and the Crown Prosecution Service (memorandum of understanding with Historic England and the National Police Chiefs' Council); Opal (heritage and cultural property crime analysis)	Physical: offences of carrying out unauthorised works to a listed building (up to two years' imprisonment and an unlimited fine) and damaging a listed building; damaging or carrying out works to a scheduled monument, and using a metal detector on a scheduled monument or in an archaeological area without consent; failure to report treasure; dealing in tainted cultural objects. Historic England provides training for police officers and prosecutors, risk assessment guidance for owners and impact statements for sentencing. Opal's research for Historic England (2020–23) found organised theft of York stone from church grounds and historic properties, lead theft from places of worship up 41 per cent during the 2020 lockdowns before falling 26 per cent in 2023, £3.2 million of cultural property stolen from museums and country houses in 2021–22, and 943 places of worship on the Heritage at Risk Register, 53 of them because of crime; it recommended a heritage crime marker on police recording systems. Cyber: none; collections and site management systems follow ordinary data protection law.	Planning (Listed Buildings and Conservation Areas) Act 1990 ss.7–9 and 59; Ancient Monuments and Archaeological Areas Act 1979 ss.2, 28 and 42; Treasure Act 1996 (definition of treasure widened from 30 July 2023); Dealing in Cultural Objects (Offences) Act 2003; Protection of Wrecks Act 1973; Protection of Military Remains Act 1986; Criminal Damage Act 1971.
Places of worship (protective security and counter-terrorism)	Home Office (Places of Worship Protective Security Funding Scheme; Jewish Community Protective Security Grant administered by the Community Security Trust; Protective Security for Mosques Scheme); Counter Terrorism Policing and Counter Terrorism Security Advisers; National Protective Security Authority; Security Industry Authority (Martyn's Law); Church of England Church Buildings Council and diocesan advisory committees; Ecclesiastical Insurance and other insurers	Physical: £73.4 million of Home Office protective security funding for 2026–27 (announced 20 February 2026): up to £28.4 million for Jewish community sites, up to £40 million for mosques and Muslim faith schools, and £5 million for Christian, Hindu, Sikh and other places of worship, paying for guarding, CCTV, fencing, alarms and lighting. Under Martyn's Law, premises used principally for worship are placed in the standard tier however many people attend, so a cathedral or large church must notify the Security Industry Authority and have evacuation, invacuation and lockdown procedures but is not required to adopt enhanced-tier measures. Security works to Church of England churches (roof alarms, CCTV, replacement roofing in terne-coated steel) need faculty approval under the ecclesiastical exemption rather than listed building consent; other exempt denominations have equivalent internal systems. Cyber: none specific; UK General Data Protection Regulation for congregation data.	Terrorism (Protection of Premises) Act 2025 (standard tier for places of worship); Ecclesiastical Exemption (Listed Buildings and Conservation Areas) (England) Order 2010; Ecclesiastical Jurisdiction and Care of Churches Measure 2018 and Faculty Jurisdiction Rules 2015; Public Order Act 1986 and Crime and Disorder Act 1998 (religiously aggravated offences).
Historic environment (Wales, Scotland and Northern Ireland)	Cadw (Welsh Government); Historic Environment Scotland and the Treasure Trove Unit (Crown Office and Procurator Fiscal Service); Department for Communities Historic Environment Division (Northern Ireland); local	Physical: equivalent consent and offence regimes for listed buildings and scheduled monuments in each nation. Wales consolidated its heritage law in the Historic Environment (Wales) Act 2023, in force from 4 November 2024. Scotland's regime rests on the Historic Environment Scotland Act 2014 and its planning and ancient monuments legislation, with all ownerless finds subject to treasure trove and the Crown. Northern Ireland scheduling and listing	Historic Environment (Wales) Act 2023; Historic Environment Scotland Act 2014; Ancient Monuments and Archaeological Areas Act 1979 (Scotland and Wales); Planning (Listed Buildings and

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
	planning authorities; Police Scotland, Police Service of Northern Ireland and Welsh police forces	sit with the Department for Communities. Heritage Watch and ARCH-style partnerships operate in each nation through the police and the heritage bodies. Cyber: none.	Conservation Areas (Scotland) Act 1997; Historic Monuments and Archaeological Objects (Northern Ireland) Order 1995; Planning Act (Northern Ireland) 2011.
National heritage estates, museums and collections (National Trust, English Heritage, cathedrals, country houses, museums and galleries)	No security regulator. Arts Council England (Government Indemnity Scheme security requirements; museum Accreditation); Department for Culture, Media and Sport; National Trust, English Heritage and the Church Commissioners as owners; Historic England and ARCH; police and Opal; insurers; the Art Loss Register and Interpol databases for stolen cultural property	Physical: security standards are contractual or conditions of grant, indemnity and insurance rather than statutory; the Government Indemnity Scheme requires borrowers to meet national security standards for loans, and Accreditation requires documented security and emergency planning. Theft from historic houses and museums is prosecuted as burglary or theft, with the cultural value of the property as an aggravating factor; export of stolen or unlawfully removed cultural objects is controlled by Arts Council England export licensing. Cyber: collections databases and visitor systems are subject to UK General Data Protection Regulation only.	Dealing in Cultural Objects (Offences) Act 2003; Cultural Property (Armed Conflicts) Act 2017; Export Control Act 2002 and the Export of Objects of Cultural Interest (Control) Order 2003; Museums and Galleries Act 1992; National Heritage Act 1983 (Historic England, and English Heritage's predecessor); National Trust Acts 1907–1971.

6.4 Freight and transport crime: cargo theft on road, rail, air and sea

Nobody leads on freight crime in the way that the Environment Agency leads on waste or Historic England on heritage. The Home Office owns the policy, the Department for Transport owns the road network and lorry parking, the National Police Chiefs' Council has a lead for vehicle crime, and Opal analyses serious organised acquisitive crime, but there is no freight crime offence, no Home Office crime code and no national strategy.

The practical lead is the National Vehicle Crime Intelligence Service's freight desk, a police unit funded entirely by industry, working with the trade associations, insurers and the Transported Asset Protection Association's voluntary standards.

Food and drink are consistently among the most-stolen product categories in the Association's European incident data, and the cold-chain and logistics row in Section 5.1 should be read with this subsection.

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
Road freight: goods in transit, trailers, lorry parks, laybys, motorway services and distribution centres	No statutory security regulator. Police forces (offences recorded as theft from a vehicle; West Midlands Police piloting a freight crime flag for national roll-out); National Vehicle Crime Intelligence Service (NaVCIS) Freight (industry-funded police unit; holds the UK Freight Crime	Physical: no security requirement attaches to a goods vehicle operator's licence, a warehouse or a lorry park. Protection rests on voluntary standards and insurer conditions: the Transported Asset Protection Association (TAPA) Facility, Trucking and Parking Security Requirements (FSR, TSR and PSR), Park Mark Freight accreditation for lorry parks (British Parking Association with Police Crime Prevention Initiatives), Secured by Design for new sites, and the Road Haulage Association	Theft Act 1968; Fraud Act 2006; Goods Vehicles (Licensing of Operators) Act 1995; Sentencing Council, Theft Offences: Definitive Guideline (2016); Crime and

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
	database; no Home Office funding); Opal (serious organised acquisitive crime intelligence); National Police Chiefs' Council lead for vehicle crime and the National Vehicle Crime Reduction Partnership; National Business Crime Centre; Home Office (policy; National Vehicle Crime Working Group); Department for Transport and National Highways (lorry parking; match-funding schemes 2022 and 2023); Traffic Commissioners and Driver and Vehicle Standards Agency (operator licensing only)	and Logistics UK guidance. NaVCIS recorded 3,424 freight crime notifications in 2025 (nine a day) with £65.1 million of goods stolen, 54 per cent from laybys and industrial estates and 20 per cent from motorway services, curtain-slashing being the commonest method; it supported more than 40 operations leading to 265 arrests. The Road Haulage Association put 2024 losses at £111 million, and the All-Party Parliamentary Group for Freight and Logistics ('Securing our supply chains', November 2024) estimated the true annual cost at £680 to £700 million and called for a national strategy, secure parking standards and planning reform. Cyber: load fraud through online freight exchanges (fictitious carriers collecting genuine loads), theft of telematics and tracking credentials and ransomware against logistics platforms; no regulator and no reporting duty beyond personal data breaches.	Policing Act 2026 s.149 (electronic devices used in vehicle theft); Freight Crime Bill 2024–26 (ten-minute rule Bill, Rachel Taylor MP: recording and investigation of freight crime; further stages awaited).
Food and drink in the distribution network (cold chain, regional distribution centres, third-party logistics, delivery fleets)	As above, with the Food Standards Agency National Food Crime Unit (stolen or diverted food re-entering the chain is food crime); Defra Food Supply Chain Resilience team and Food Resilience Industry Forum; local authority environmental health (temperature control); insurers and retailer supplier standards	Physical: food and drink is among the most frequently stolen product categories in TAPA's European incident data and features in NaVCIS's seasonal peaks (alcohol before Christmas, chilled and ambient groceries year-round); stolen loads are typically sold through informal retail or re-labelled, which makes the National Food Crime Unit a relevant investigator as well as the police. The supermarket distribution model concentrates risk in a small number of regional distribution centres and contracted haulage fleets, and the 2025 retail ransomware incidents showed how quickly a logistics platform outage empties shelves. Security expectations come from retailer and Brand Reputation Compliance Global Standards audit requirements rather than law (see Section 5.1). Cyber: as above; the National Cyber Security Centre's supply-chain guidance is advisory only.	Food Safety Act 1990 and retained Regulation (EC) 178/2002 (traceability, withdrawal and recall); Food Hygiene (England) Regulations 2013; Theft Act 1968; Fraud Act 2006.
Rail freight and intermodal terminals	British Transport Police; Department for Transport Land Transport Security (National Railway Security Programme, which applies to freight operators and terminals); Network Rail; Office of Rail and Road (safety); freight operating companies	Physical: rail freight and terminals sit inside the statutory rail security regime (Section 10.1), so operators must comply with the National Railway Security Programme; British Transport Police investigates theft from wagons and terminals and cable theft on the network. Cyber: Department for Transport is the Network and Information Systems Competent Authority for designated rail operators.	Railways Act 1993 s.119; Railways and Other Guided Transport Systems (Safety) Regulations 2006; Network and Information Systems Regulations 2018.
Air cargo: regulated agents, known consignors and cargo handlers	Civil Aviation Authority (aviation security regulator; validates and lists regulated agents and known consignors, CAP 1179); Department for Transport (National Aviation Security Programme and directions); Border Force and HM Revenue and Customs	Physical: the only fully statutory cargo security regime in the UK. Cargo may only be loaded as 'secure' if it has been screened by a regulated agent or originated with a known consignor whose premises, processes and staff training have been validated by Civil Aviation Authority auditors, with revalidation every twelve months; failure is a criminal offence and grounds for removal from the list. Cyber: covered by the joint Department for	Aviation Security Act 1982; Aviation and Maritime Security Act 1990; Civil Aviation Act 2012; retained Regulation (EC) 300/2008 and Implementing Regulation (EU)

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
	(customs and prohibited goods)	Transport and Civil Aviation Authority Network and Information Systems regime and CAP 1753 (Section 10.3).	2015/1998; Single Consolidated Direction (Department for Transport).
Sea freight: ports, container terminals and roll-on roll-off traffic	Department for Transport Maritime Security (International Ship and Port Facility Security Code and Port Security Regulations 2009); port police forces and port operators; Border Force and HM Revenue and Customs; National Crime Agency (organised smuggling); Maritime and Coastguard Agency	Physical: port facility security plans, access control and restricted areas under the International Ship and Port Facility Security regime (Section 10.4) protect the port estate rather than the cargo owner's goods; theft of containers and of goods from trailers awaiting shipment falls to port police and the local force, and cargo crime at ports is part of the National Vehicle Crime Reduction Partnership's port resilience priority. Cyber: Department for Transport is the Network and Information Systems Competent Authority for designated harbour authorities and terminal operators; the Ports and Port Systems Cyber Security Code of Practice is advisory.	Ship and Port Facility (Security) Regulations 2004; Port Security Regulations 2009; Customs and Excise Management Act 1979; Network and Information Systems Regulations 2018.
Freight crime partnerships and standards bodies (non-statutory)	Transported Asset Protection Association (TAPA) EMEA (industry association; FSR, TSR and PSR certification standards; TAPA Intelligence System replacing the Incident Information Service since 2022); Road Haulage Association and Logistics UK (campaigns for a freight crime offence, a crime code and public funding for NaVCIS); British International Freight Association; TT Club and other cargo insurers; British Parking Association (Park Mark Freight); European Secure Parking Organisation; All-Party Parliamentary Group for Freight and Logistics	Physical: these bodies set the standards that insurers and customers require, run the incident databases that fill the gap left by police recording, and lobby for statutory recognition. In June 2026 TAPA recorded 224 UK incidents in a single month, placing the UK fifth in Europe. The Home Office has agreed to pilot a freight crime flag on police recording systems rather than a dedicated crime code; the Road Haulage Association's 2024 manifesto asked police and crime commissioners to include freight crime in their plans and to fund NaVCIS operations. Cyber: none.	No statutory basis; TAPA standards are contractual certification schemes. Freight Crime Bill 2024–26.

6.5 What this means for rural estates

For a rural estate the practical consequences are four.

- First, the scrap metal licensing regime is only as strong as local enforcement, and it does not extend to Northern Ireland; estates suffering repeat metal theft should ask their local authority licensing team and the National Infrastructure Crime Reduction Partnership what checks are being made on mobile collectors, and should mark lead, copper and machinery forensically so that stolen material can be traced when a yard is inspected.
- Second, fly-tipping law places the clearance burden on the occupier, so gates, barriers, cameras and prompt reporting to the local authority (which can then use its fixed penalty and vehicle seizure powers, and from commencement of the Crime and Policing Act 2026 the penalty points

sanction) are the only ways of shifting the cost back onto the offender; the waste carrier reforms should make it easier to identify rogue operators once the permit register is live.

- Third, for churches and heritage assets the protective measures that work (roof alarms, forensic marking, replacement roofing, lighting and Heritage Watch reporting) are almost all voluntary or insurer-driven, and the public funding that does exist is directed at counter-terrorism rather than acquisitive crime; Rural SafeGuard's view is that the heritage crime marker recommended by Opal and Historic England, and its adoption by all forces, would do more than any new offence to make this crime visible and resourced.
- Fourth, freight crime is the gap most likely to reach a farm or estate indirectly, through the haulier, cold store or distribution centre that carries its produce; until a freight crime offence or crime code exists, the useful levers are contractual (requiring TAPA or Park Mark Freight accredited parking and facilities in haulage and storage contracts), reporting every theft to the police with the NaVCIS #FREIGHT tag so that it reaches the national database, and supporting the industry's case for public funding of NaVCIS.

7. Rural land uses and rural crime regimes

Rural SafeGuard's purpose is to bring the security practice of the industrial sectors to farmers, landowners, insurers and rural communities.

Sections 8 to 14 describe the regulated networks; this section covers the land uses and activities that share the same characteristics (isolation, high-value portable assets, thin policing and a dependence on the owner's own measures) but that the critical national infrastructure framework never reaches:

- construction sites and the plant on them,
- the solar, wind and battery sites now scattered across farmland,
- the car boot sales and markets that landowners host, woodland and timber, rivers and fisheries, and
- the wildlife, livestock, equine, pet and firearms regimes that define rural policing.

It ends with the bodies that set rural crime policy and produce the figures, because knowing who counts a crime is usually the first step to getting it resourced.

The pattern of the earlier sections repeats. Where a statutory regime exists, it is there for safety, planning, animal health or conservation rather than security, and the security benefit is a by-product: the Health and Safety Executive requires construction sites to keep unauthorised people out because they might be hurt, not because plant might be stolen; the Forestry Commission licenses felling to protect woodland, not to stop timber theft; the Environment Agency polices rod licences to conserve fish stocks.

Policing is delivered through small national units funded partly by the industries they protect, and the industry bodies do the recording that the police do not.

7.1 Construction sites, plant theft and remote energy sites

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
Construction sites in rural areas (housing, infrastructure, energy and utility works, farm building projects)	Health and Safety Executive (site safety, including the duty to prevent unauthorised access); local planning authorities (planning conditions on hours, lighting, fencing and construction management plans); police forces; no security regulator	Physical: the Construction (Design and Management) Regulations 2015 require the principal contractor to take reasonable steps to prevent unauthorised access to a site, which is the only statutory site-security duty and exists for safety reasons; Secured by Design's construction guidance and insurer conditions supply the rest. Rural sites share the farm's risk profile: remote, unoccupied at night, full of portable high-value plant, fuel and copper, and served by roads with no natural surveillance. Cyber: none; site telematics, access-control and camera systems are unregulated connected devices (Section 5.2).	Construction (Design and Management) Regulations 2015 reg.13(4) (unauthorised access); Health and Safety at Work etc. Act 1974; Occupiers' Liability Acts 1957 and 1984; Town and Country Planning Act 1990 (conditions).
Construction plant and agricultural machinery theft (excavators, telehandlers, generators, compressors, tools, trailers,	Police forces; National Construction and Agricultural Theft Team (NCATT, hosted by Northumbria Police since 2021, funded by industry donations; founder Andy Huddleston returned as civilian head in December 2025); National Rural Crime	Physical: no statutory marking or immobiliser requirement yet applies. The Equipment Theft (Prevention) Act 2023 allows regulations to require forensic marking, immobilisers and registration on new equipment; the Home Office's October 2025 response confirmed regulations for forensic marking and database registration of new all-terrain vehicles and GPS units only, dropping immobilisers because of type-approval concerns, and the regulations had not been made at the date of this guide. The Crime and Policing Act 2026 gives	Equipment Theft (Prevention) Act 2023 (regulations awaited); Crime and Policing Act 2026 (entry to recover electronically tracked stolen goods); Theft Act 1968; Scrap Metal

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
GPS units, quad bikes)	Unit; National Vehicle Crime Intelligence Service agriculture and plant desk; Opal; Combined Industries Theft Solutions (CITS, the police, insurer, hire and manufacturer partnership); Construction Equipment Association (CEA) and Agricultural Engineers Association (CESAR scheme with Datatag); Construction Plant-hire Association; The Equipment Register; Home Office	police a power to enter premises without a warrant to recover stolen goods carrying an electronic tracker. NFU Mutual recorded agricultural vehicle theft up 18 per cent to £8.3 million and quad and all-terrain vehicle theft up 31 per cent to £3.5 million in 2025, while GPS unit theft fell 80 per cent. CITS is the industry body that convenes police, insurers, hirers and manufacturers on plant theft; NCATT is the police unit that investigates it; CESAR is the marking and registration scheme that makes recovery possible. Cyber: telematics and immobiliser systems are manufacturer-controlled and unregulated.	Dealers Act 2013 (Section 6.1); Road Traffic Act 1988 and vehicle registration law for road-going plant.
Remote energy sites on farmland (solar farms, onshore wind, battery energy storage, private-wire and grid connections, substations)	Ofgem (licensed generators and network operators only; most solar and wind farms operate under licence exemptions); Department for Energy Security and Net Zero and Ofgem as Network and Information Systems Competent Authority (designated operators only, Section 8.1); Health and Safety Executive (electrical safety; battery storage fire and explosion hazards, with fire and rescue services); local planning authorities (planning conditions, decommissioning bonds); police forces; Solar Energy UK and RenewableUK (trade bodies); insurers	Physical: no security requirement attaches to a solar, wind or battery site unless its operator is licensed and designated under the Network and Information Systems regime, which few are. Cable theft is the dominant crime: industry reporting recorded more than 750 kilometres of cable stolen from UK solar sites between January and August 2024, with a further surge in spring 2025 across Dorset, Sussex, Essex, Derbyshire, Lancashire, Worcestershire and Staffordshire, and thefts are often carried out with vehicles and cutting equipment over several nights on unmanned sites. Panel theft, inverter theft and vandalism follow. Protection depends on planning conditions, perimeter detection, forensic marking of cable and the landowner's lease terms; the national grid and distribution networks that these sites feed are regulated (Section 8) but the sites themselves are not. Cyber: inverters, battery management systems and monitoring platforms are internet-connected operational technology, mostly foreign-manufactured, with no UK product-security requirement (Section 5.2); the Department for Energy Security and Net Zero's 2026 consultation proposes bringing non-licensed downstream participants within the Network and Information Systems regime.	Electricity Act 1989 (licensing and exemptions; Electricity (Class Exemptions from the Requirement for a Licence) Order 2001); Network and Information Systems Regulations 2018 (designated operators only); Electricity Safety, Quality and Continuity Regulations 2002; Town and Country Planning Act 1990; Theft Act 1968.

7.2 Car boot sales, markets and events on private land

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
Car boot sales, temporary markets, fairs and events on private land (England and Wales)	Local planning authority (temporary use of land); local authority markets and licensing functions (market franchise rights, street trading where a local Act applies, event safety	Physical: there is no national licence for a car boot sale. A landowner may use land for a market for up to 14 days a year (28 days for other temporary uses) under permitted development rights, after which planning permission is needed; a council with historic market rights may require its consent or charge for events within six and two-thirds miles of its own market; food sellers must be registered; and charitable sales need a	Town and Country Planning (General Permitted Development) (England) Order 2015, Schedule 2 Part 4 Class B (temporary use of land: 28 days, or 14

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
	advisory groups); Trading Standards (counterfeit and unsafe goods, the 'Real Deal' charter); environmental health (food hygiene registration); police (stolen goods, disorder, traffic); Charity Commission and local authority (charitable collections); no licensing regime	collection permit. Private sellers at a car boot sale are outside consumer protection law, second-hand goods are not recorded, and there is no requirement to identify sellers, which is why tools, garden machinery, bicycles, quad parts and farm items stolen in the countryside are commonly disposed of there. Trading Standards and police 'days of action' target counterfeit and stolen goods, but the burden of preventing a sale from becoming an outlet for stolen property falls on the landowner and operator through their entry conditions, seller registration and cooperation with the police. Landowners also carry occupiers' liability for visitors and the duty of care for waste left behind (Section 6.2). Cyber: none; online marketplaces are regulated separately by the Online Safety Act 2023 and consumer law.	days for markets); Food Act 1984 s.37 (market franchise rights); Local Government (Miscellaneous Provisions) Act 1982 Schedule 4 (street trading, where adopted); Food Hygiene (England) Regulations 2013; Police, Factories, etc. (Miscellaneous Provisions) Act 1916 (street collections); Consumer Protection Act 1987 and Consumer Rights Act 2015 (traders only); Theft Act 1968 s.22 (handling); Occupiers' Liability Acts 1957 and 1984.
Markets and second-hand dealing (Scotland and Northern Ireland)	Scotland: local authorities (market operator's licence and second-hand dealer's licence under the Civic Government (Scotland) Act 1982); Police Scotland; Trading Standards. Northern Ireland: district councils (street trading licences; market rights); Police Service of Northern Ireland; Trading Standards Service (Department for the Economy)	Physical: Scotland is the only part of the UK that licenses car boot sales as such. A market operator's licence is required for any private market, explicitly including car boot sales, craft fairs and fêtes, unless the event is not run for private profit or is confined to livestock, fodder or grain, and councils attach conditions on layout, hours and public safety; second-hand dealers must be licensed and keep records. Northern Ireland has street trading licensing and council market rights but no car boot sale licence. Cyber: none.	Civic Government (Scotland) Act 1982 ss.24–27 (second-hand dealers) and s.40 (market operators); Street Trading Act (Northern Ireland) 2001.

7.3 Forestry, woodland and timber

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
Woodland, forestry operations and timber (commercial forests, farm woodland, ancient woodland, Christmas tree plantations, timber in transit)	Forestry Commission (England: felling licences, restocking and enforcement notices, National Enforcement team) and Forestry England (public forest estate); Scottish Forestry and Forestry and Land Scotland; Natural Resources Wales; Forest Service (Department of Agriculture, Environment and Rural Affairs, Northern Ireland); Office for Product	Physical: the statutory regime is a licensing one. Felling more than five cubic metres in a calendar quarter needs a felling licence, and since January 2023 unlicensed felling in England carries an unlimited fine, court-ordered restocking with ten years' maintenance, and restocking and enforcement notices that bind successors in title and are registered as local land charges. Theft of standing or felled timber, Christmas trees, firewood, fencing and chainsaws and forestry plant is prosecuted as ordinary theft and reported to the police, not to the Forestry Commission; the Commission's online	Forestry Act 1967 as amended by the Environment Act 2021 Schedule 16 (unlimited fines, s.24B restocking orders, s.17A and s.24 notices); Forestry (Felling of Trees) Regulations 1979; Timber and Timber Products (Placing on the Market) Regulations

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
	Safety and Standards (UK Timber Regulation, illegally harvested timber placed on the market); police forces and the National Wildlife Crime Unit (protected species and habitats); local planning authorities (tree preservation orders); Confor and the Royal Forestry Society (industry bodies); no security regulator	reporting route covers suspected illegal felling only. Illegally harvested timber is a market offence under the UK Timber Regulation enforced by the Office for Product Safety and Standards. Woodland is also the setting for much of the fly-tipping, off-road vehicle and poaching activity covered elsewhere in this guide. Cyber: none; forestry operations increasingly rely on satellite-guided harvesters and drone survey systems that fall within the machinery gap in Section 5.2.	2013 (UK Timber Regulation); Forestry and Land Management (Scotland) Act 2018; Forestry Act (Northern Ireland) 2010; Town and Country Planning Act 1990 Part VIII (tree preservation); Theft Act 1968.

7.4 Rivers, angling and inland fisheries

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
Rivers, lakes and stillwater fisheries (England and Wales): rod licensing, poaching, fish theft and illegal netting	Environment Agency (fisheries regulator and enforcement body in England: rod licences, byelaws, close seasons, fisheries enforcement officers with statutory powers); Natural Resources Wales (Wales); Angling Trust (Fisheries Enforcement Support Service, funded by the Environment Agency, and the volunteer network that replaced the Voluntary Bailiff Service in May 2026); police forces and the National Wildlife Crime Unit (poaching is a priority wildlife crime); Institute of Fisheries Management; fishery owners and angling clubs (private bailiffs)	Physical: fishing without a rod licence, fishing in the close season (15 March to 15 June on rivers) and breaching byelaws are offences enforced by Environment Agency officers, who can seize equipment and prosecute; taking or destroying fish in private waters is theft under Schedule 1 of the Theft Act 1968, and organised removal of carp and other specimen fish from stillwater fisheries, illegal netting of salmon, sea trout and eels, and the theft of fish for sale are investigated by the police with Environment Agency support. The Environment Agency reports that more than half of illegal fishing reports come through Angling Trust volunteers; the annual Operation Clampdown patrols the close season, and Angling Alert provides a national reporting tool. Fishery owners hosting day-ticket or syndicate waters rely on their own bailiffs, ticket conditions and the Angling Trust's guidance. Cyber: none; fishery booking and licensing systems are ordinary data-protection matters.	Salmon and Freshwater Fisheries Act 1975; Environment Act 1995 (Environment Agency fisheries functions) and Marine and Coastal Access Act 2009 Part 7 (byelaw and enforcement powers); Theft Act 1968 Schedule 1 para.2 (taking or destroying fish); Eels (England and Wales) Regulations 2009; Salmon Act 1986 (handling salmon in suspicious circumstances).
Inland fisheries (Scotland and Northern Ireland)	Scotland: Marine Directorate (Scottish Government), District Salmon Fishery Boards (statutory bodies with their own water bailiffs), Fisheries Management Scotland, Police Scotland; no rod licence, but a permit from the proprietor is required. Northern Ireland: Department of Agriculture, Environment and Rural Affairs Inland Fisheries (rod licences and enforcement) and the Loughs Agency (Foyle and Carlingford catchments); Police Service of Northern Ireland	Physical: in Scotland the District Salmon Fishery Boards' bailiffs hold statutory powers to search, seize and report offenders for salmon and sea trout poaching, and fishing for salmon without written permission is a criminal offence; freshwater fish protection rests on the Wildlife and Natural Environment (Scotland) Act 2011. In Northern Ireland fishery protection officers of the Department and the Loughs Agency enforce licensing and close seasons. Cyber: none.	Salmon and Freshwater Fisheries (Consolidation) (Scotland) Act 2003; Aquaculture and Fisheries (Scotland) Act 2007; Fisheries Act (Northern Ireland) 1966; Foyle Fisheries Act (Northern Ireland) 1952.

7.5 Wildlife, livestock, horses, pets and firearms

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
Wildlife crime: hare coursing, poaching, badger, bat and bird of prey offences, illegal hunting, egg and specimen collecting	Police forces (rural crime and wildlife crime officers); National Wildlife Crime Unit (NWCU, £450,000 Home Office and Defra funding 2025–26); Crown Prosecution Service (specialist wildlife prosecutors); Natural England, NatureScot, Natural Resources Wales and the Northern Ireland Environment Agency (licensing and advice); Royal Society for the Protection of Birds investigations; Partnership for Action Against Wildlife Crime; Border Force (trade in endangered species)	Physical: hare coursing is now addressed by the dedicated offences in the Police, Crime, Sentencing and Courts Act 2022 (trespass with intent to search for or pursue hares with dogs, and going equipped), with unlimited fines, up to six months' imprisonment, dog disqualification and kennelling-cost recovery orders, and a Sentencing Council guideline in force from 1 June 2026. Hare coursing and poaching gangs are recognised as organised, mobile and linked to intimidation of farmers, which is why the National Police Chiefs' Council strategy treats them alongside machinery theft. Protected species offences (badger sett interference, bat roost destruction, raptor persecution) are enforced through the Wildlife and Countryside Act 1981 and the Protection of Badgers Act 1992 with the National Wildlife Crime Unit providing intelligence and case support. Cyber: none, though online sales of specimens and eggs are monitored.	Wildlife and Countryside Act 1981; Protection of Badgers Act 1992; Hunting Act 2004; Game Act 1831 and Night Poaching Act 1828; Police, Crime, Sentencing and Courts Act 2022 ss.63–65; Deer Act 1991; Conservation of Habitats and Species Regulations 2017; Wildlife and Natural Environment (Scotland) Act 2011 and Wildlife Management and Muirburn (Scotland) Act 2024; Wildlife (Northern Ireland) Order 1985.
Livestock theft, livestock worrying and animal identification	Police forces and the National Rural Crime Unit; Animal and Plant Health Agency and Rural Payments Agency (identification, movement records and the Livestock Information Service); local authority trading standards (animal health enforcement); Defra; National Farmers' Union, NFU Mutual and the National Sheep Association	Physical: insurance claims for livestock theft rose 30 per cent to £4.5 million in 2025 (one specialist insurer - NFU Mutual). Statutory identification and movement recording (ear tags, cattle passports, the Livestock Information Service for sheep, goats and deer) exist for disease control but are the main tool for tracing stolen animals through markets and abattoirs, where the Food Standards Agency and local authorities check identification. The Dogs (Protection of Livestock) (Amendment) Act 2025, in force since 18 March 2026, extends the livestock worrying offence to roads and paths and to camelids, removes the £1,000 cap on fines, and gives police powers to seize dogs, enter premises under warrant and take DNA and dental samples. Cyber: the Livestock Information Service and cattle tracing systems are Defra and Animal and Plant Health Agency systems assured under GovAssure (Section 5.1).	Theft Act 1968; Dogs (Protection of Livestock) Act 1953 as amended by the Dogs (Protection of Livestock) (Amendment) Act 2025; Animal Health Act 1981; Sheep and Goats (Records, Identification and Movement) (England) Order 2009; Cattle Identification Regulations 2007; Livestock Identification and Movement rules of the devolved administrations.
Horses, ponies and pets (equine theft, dog and cat abduction, tack and horsebox theft)	Police forces; Defra (equine identification and the Central Equine Database); local authorities (animal welfare licensing); Horsecatch groups and the British Horse Society; Pet Theft Taskforce successor arrangements; microchip database operators	Physical: every horse must have a passport and, since October 2020, a microchip recorded on the Central Equine Database, which is the practical tool for recovering stolen animals; horseboxes, trailers and tack are treated as ordinary theft, with trailer theft a persistent rural problem. The Pet Abduction Act 2024 created specific offences of dog and cat abduction (up to five years' imprisonment) in England and Northern Ireland, in force since 24 August 2024, and a power to extend to other species. Cyber: none.	Equine Identification (England) Regulations 2018 and equivalents in the devolved nations; Pet Abduction Act 2024; Microchipping of Cats and Dogs (England) Regulations 2023; Animal Welfare Act 2006; Theft Act 1968.

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
Firearms, shotguns and shooting estates	Chief officers of police (firearm and shotgun certificates, suitability, security of storage); Home Office (statutory guidance to chief officers, Firearms Security Handbook); His Majesty's Inspectorate of Constabulary and Fire & Rescue Services (inspection of licensing); British Association for Shooting and Conservation and the Countryside Alliance (industry bodies); National Crime Agency and the National Firearms Targeting Centre (criminal use)	Physical: firearms licensing is the one rural regime that is unambiguously about security. Certificate holders must store firearms and ammunition to the standards in the Home Office Firearms Security Handbook (2020) as a condition of the certificate, police firearms enquiry officers inspect storage, and theft of a firearm must be reported immediately; the Home Office statutory guidance (2021, revised 2023) governs suitability checks, and further licensing reforms were consulted on in 2024–25. Estates, gamekeepers and registered firearms dealers hold concentrations of weapons that make them targets, and gun cabinets, keys and vehicles carrying firearms are the usual points of loss. Cyber: none specific; the police National Firearms Licensing Management System and dealer registers are government systems.	Firearms Act 1968 and Firearms (Amendment) Acts 1988 and 1997; Firearms Rules 1998; Policing and Crime Act 2017 Part 6; Offensive Weapons Act 2019; Home Office Statutory Guidance to Chief Officers of Police (2021, revised 2023); Firearms Security Handbook 2020.

7.6 Rural crime governance and the bodies that count it

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
National policing structures for rural crime	National Police Chiefs' Council lead for Rural and Wildlife Crime (Deputy Chief Constable Nigel Harrison); National Rural Crime Unit (£365,000 funding 2025–26); National Wildlife Crime Unit (£450,000); National Construction and Agricultural Theft Team; National Vehicle Crime Intelligence Service (agriculture, plant and freight desks); Opal; Home Office (funding and policy); police and crime commissioners and the National Rural Crime Network; Scottish Partnership Against Rural Crime; Wales rural crime teams; Police Service of Northern Ireland Rural Crime Unit	Physical: the National Police Chiefs' Council Rural and Wildlife Crime Strategy 2025–2028, launched on 25 November 2025, sets nine priorities: machinery theft, livestock worrying and theft, illegal hunting and poaching, offences against protected species, hare coursing, fly-tipping, waste crime, domestic abuse and sexual violence in rural areas, and rural mental health. It commits forces to intelligence-led policing, crime mapping and drone support, and reported £12.7 million of stolen machinery recovered and 155 arrests in its first year. There is no separate Home Office rural crime strategy; the small national units depend on annual Home Office grants and industry contributions, and the Commons Library's 2025 briefing notes that recording of rural crime remains inconsistent between forces. Cyber: the National Cyber Security Centre and National Farmers' Union guidance for farmers is the only rural-specific cyber material.	No statutory basis for the strategy; Police Reform and Social Responsibility Act 2011 (police and crime commissioners' plans); Crime and Policing Act 2026 (new powers used by the strategy).
Industry bodies and the rural crime figures	NFU Mutual (annual Rural Crime Report, the only consistent national cost series); National Farmers' Union, NFU Cymru, NFU Scotland and the Ulster Farmers' Union; Country Land and Business Association; Countryside Alliance; British Association for Shooting and Conservation; Combined	Physical: NFU Mutual's Rural Crime Report 2026 (28 May 2026) put the cost of rural crime related claims payouts by them in 2025 at £41.5 million, down 6 per cent, with the Midlands and Wales down 21 per cent but Northern Ireland up 24 per cent, Scotland up 14 per cent and the Northeast up 7 per cent, and 29 per cent of its agents reporting farmers changing practice or leaving farming because of crime. Because police recorded-crime statistics have no rural flag, the	No statutory basis.

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
	Industries Theft Solutions; Agricultural Engineers Association and Construction Equipment Association (CESAR); Angling Trust; Confor; Historic England (heritage); Crimestoppers Rural; Neighbourhood, Farm and Horse Watch networks	insurer's claims data, the industry incident databases described in Sections 6 and 7, and the National Rural Crime Network's surveys are what policy is built on. Rural SafeGuard's assessed-property programme sits alongside these bodies as a crime risk reduction standard rather than a recording one. Cyber: none.	

Taken together, Sections 5 to 7 and 14 describe a countryside in which almost every asset is regulated for something and almost none for security.

The gaps that matter most to Rural SafeGuard's members are consistent:

- no statutory security duty on the owner of a farm, a construction site, a solar farm, a woodland or a fishery; national policing units that are small, grant-funded and dependent on industry;
- crime recording that cannot distinguish rural, freight, heritage or plant crime from the general theft figures; and
- a set of licensing regimes (scrap metal, waste carriers, felling, rod licences, firearms, markets in Scotland) whose enforcement is the real control on the end market for stolen property.

The practical response is the one this guide has argued throughout:

- use the regulated regimes where they reach,
- report to the licensing authority as well as the police,
- insist on accredited standards in contracts and leases,
- mark and register everything that can be marked, and
- give the industry bodies the incident data that lets them make the case for the rest.

8. Energy networks

Sections 8 to 14 describe the regulated critical national infrastructure networks that the rural estate hosts and depends on. They are the benchmark against which the gaps in Sections 5 to 7 should be judged: each has a responsible department, a competent authority, a security standard and a reporting duty. Lead Government Department for energy: Department for Energy Security and Net Zero (DESNZ). The Energy Emergencies Executive Committee (E3C), co-chaired by the Department and industry, coordinates sector resilience. The Energy Sector Cyber Security Strategy, published on 28 May 2026 by the Department, the National Cyber Security Centre, Ofgem and the National Energy System Operator (NESO), describes the four 'Quad partners' that lead energy cyber regulation and resilience.

8.1 Electricity (transmission, distribution, generation, interconnectors, system operation)

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
Great Britain electricity networks, generators and system operator	Department for Energy Security and Net Zero (DESNZ) (Secretary of State) and Ofgem (Gas and Electricity Markets Authority), jointly	Cyber: joint Network and Information Systems (NIS) Competent Authority. Ofgem delivers guidance, Cyber Assessment Framework (CAF)-based assurance, inspections, enforcement and penalties; DESNZ sets policy and risk appetite. Physical: DESNZ as Lead Government Department (LGD) with National Protective Security Authority (NPSA); Ofgem licence conditions on security and resilience.	NIS Regulations 2018, Sch.1. Electricity Act 1989 (licensing; s.34 emergency directions; s.96 civil emergency powers). Energy Act 2023. DESNZ/Ofgem consultation (closed 22 May 2026) proposes extending NIS to non-licensed downstream participants and a Cyber Essentials-based baseline for all Ofgem licensees.
National Energy System Operator (NESO)	Ofgem (licence); DESNZ	Whole-system resilience coordination, advice to DESNZ/Ofgem on which services are critical; itself an Operator of Essential Services.	Energy Act 2023 (NESO established 1 October 2024).
Electricity interconnectors (subsea, to Ireland and continental Europe)	Ofgem (interconnector licence); DESNZ; Maritime and Coastguard Agency (MCA) / Crown Estate for the marine route	Cyber: NIS via DESNZ/Ofgem. Physical: licence and LGD oversight; subsea assets covered by the proposed undersea infrastructure legislation (see 11.2).	Electricity Act 1989 s.6(1)(e). Marine and Coastal Access Act 2009 (marine licence).
Offshore wind and offshore transmission owners (OFTOs)	Ofgem (generation and OFTO licences); DESNZ; Marine Management Organisation / Marine Directorate (Scotland); Maritime and Coastguard Agency; Health and Safety Executive (HSE)	Cyber: NIS via DESNZ/Ofgem where designated Operators of Essential Services (OES). Physical: LGD oversight; HSE for offshore work safety; MCA for navigational safety zones and marking.	Electricity Act 1989 s.36 consents; Energy Act 2004 (Renewable Energy Zone, safety zones s.95); Marine and Coastal Access Act 2009; Crown Estate / Crown Estate Scotland seabed leases.
Northern Ireland electricity	Department of Finance (NI) — NIS Competent Authority (CA); Utility Regulator (economic/licensing); Department for the Economy (NI) — LGD	Cyber: Department of Finance (DoF) is NIS Competent Authority for energy in NI. Physical: Department for the Economy (DfE) with NPSA.	NIS Regulations 2018, Sch.1. Electricity (NI) Order 1992.

8.2 Gas (downstream transmission, distribution, storage, liquefied natural gas terminals)

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
GB gas transmission and distribution networks, storage, liquefied natural gas (LNG) import terminals	Department for Energy Security and Net Zero (DESNZ) and Ofgem jointly (Network and Information Systems (NIS)); DESNZ alone for certain essential services; Health and Safety Executive (HSE) for gas safety and major hazards	Cyber: joint NIS Competent Authority (CA) as for electricity. Physical/integrity: HSE (Gas Safety (Management) Regulations 1996, Control of Major Accident Hazards Regulations 2015 (COMAH) for storage and terminals, Pipelines Safety Regulations 1996); DESNZ as Lead Government Department (LGD).	NIS Regulations 2018, Sch.1. Gas Act 1986. Energy Act 1976 (emergency powers). COMAH 2015.
Northern Ireland gas	Department of Finance (NI) — NIS CA; Utility Regulator; Health and Safety Executive for Northern Ireland (HSENI)	As above for NI.	NIS Regulations 2018, Sch.1. Gas (NI) Order 1996.

8.3 Oil and upstream gas, including offshore production, pipelines and fuel supply

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
Upstream oil and gas production (onshore and UK Continental Shelf (UKCS) offshore), terminals, oil pipelines, refineries, fuel storage and distribution	Department for Energy Security and Net Zero (DESNZ) (Secretary of State) — sole Network and Information Systems (NIS) Competent Authority (CA) for oil and upstream gas; Health and Safety Executive (HSE) Energy Division; North Sea Transition Authority (NSTA); Offshore Petroleum Regulator for Environment and Decommissioning (OPRED)	Cyber: DESNZ regulates Operators of Essential Services (OES) in oil and upstream gas under NIS. Physical/safety: HSE (offshore safety cases, pipelines, Control of Major Accident Hazards Regulations 2015 (COMAH) onshore); DESNZ Lead Government Department (LGD) with National Protective Security Authority (NPSA) for protective security of terminals and refineries. NSTA (licensing, stewardship) and OPRED (environmental regulation and offshore decommissioning) are not security regulators but hold licence and consent powers over operators.	NIS Regulations 2018, Sch.1. Petroleum Act 1998 (licensing, 500 m safety zones under Petroleum Act 1987 s.21). Offshore Safety Act 1992; Offshore Installations (Offshore Safety Directive) (Safety Case) Regulations 2015; Pipelines Safety Regulations 1996; COMAH 2015. Energy Act 1976 and Energy Act 2011 (fuel emergency powers, Downstream Oil Resilience).
Downstream oil resilience (refineries, import terminals, fuel distribution)	DESNZ	Statutory powers to direct downstream oil operators to maintain resilience of fuel supply, including security measures.	Energy Act 2023 Part 8 (Downstream Oil Resilience) — enables DESNZ directions and information requirements.
Hydrogen, carbon capture and storage networks (emerging)	DESNZ; Ofgem (licensing under Energy Act 2023); HSE; NSTA (CO2 storage licensing)	Emerging regimes; security expectations follow the gas model.	Energy Act 2023 Parts 1–2; Energy Act 2008 (CO2 storage).

9. Civil nuclear

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
Civil nuclear sites, nuclear material, sensitive nuclear information, and nuclear transport by road, rail and sea (including UK-flagged vessels)	Office for Nuclear Regulation (ONR) — Civil Nuclear Security and Safeguards; Civil Nuclear Constabulary (CNC); Department for Energy Security and Net Zero (DESNZ) as Lead Government Department (LGD)	Physical and cyber: ONR is the statutory security regulator. It approves site security plans covering physical protection, personnel security, cyber security and information assurance (Security Assessment Principles, SyAPs), and regulates transport security. CNC is the armed police force protecting civil nuclear sites and material in transit.	Energy Act 2013 (ONR's security purposes); Nuclear Industries Security Regulations 2003 (as amended 2017 to strengthen cyber requirements); Energy Act 2004 (CNC and Civil Nuclear Police Authority); Anti-terrorism, Crime and Security Act 2001 Part 8. Nuclear sites are outside Network and Information Systems (NIS).
Defence nuclear	Ministry of Defence (MOD) — Defence Nuclear Safety Regulator; MOD Police	Internal MOD regulation.	MOD regulatory framework (ONR regulates some defence sites under agreement).

10. Transport networks

Lead Government Department: Department for Transport (DfT). The Department's Transport Security Directorate (formerly TRANSEC) sets and enforces the statutory aviation, maritime and land-transport security programmes, and its cyber security teams act as the Network and Information Systems Competent Authority (jointly with the Civil Aviation Authority for aviation). The Office of Rail and Road (ORR) and the Civil Aviation Authority (CAA) are the independent safety/economic regulators.

10.1 Rail (mainline, light rail and metro, Channel Tunnel)

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
Mainline rail infrastructure, train operators, metro and light rail (England, Wales, Scotland)	Department for Transport (DfT) (Secretary of State) — Network and Information Systems (NIS) Competent Authority (CA) and Land Transport Security; Office of Rail and Road (ORR); British Transport Police	Cyber: DfT is sole NIS CA for rail (Cyber Assessment Framework (CAF)-based assessments; Rail Cyber Security guidance). Physical: DfT sets the mandatory National Railway Security Programme (NRSP) and inspects compliance; British Transport Police (BTP) polices the network; ORR regulates safety (including safety-critical systems and, increasingly, cyber as a safety matter).	NIS Regulations 2018, Sch.1. Railways Act 1993 s.119 (security instructions); Railways and Other Guided Transport Systems (Safety) Regulations 2006 (ORR). Rail reform: Great British Railways under the Railways Act 2025 will become the directing mind for infrastructure and services; security duties remain with DfT.
Channel Tunnel and Channel Tunnel rail services	DfT with French counterparts; Channel Tunnel Intergovernmental Commission and Safety Authority	Physical: dedicated statutory security regime for the Fixed Link.	Channel Tunnel Act 1987; Channel Tunnel (Security) Order 1994.
Northern Ireland rail (Translink)	Department of Finance (NI) — NIS CA; Department for Infrastructure (NI)	As above for NI.	NIS Regulations 2018, Sch.1.

10.2 Road (strategic road network, tunnels, traffic control and intelligent transport systems)

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
Strategic road network and traffic management systems (England and Wales)	Department for Transport (DfT) (Secretary of State) — Network and Information Systems (NIS) Competent Authority (CA); National Highways (operator, government-owned company); Welsh Government (Welsh trunk roads)	Cyber: DfT is NIS CA for road transport operators in England and Wales (intelligent transport systems, traffic control, tunnel control). Physical: DfT Lead Government Department (LGD) with National Protective Security Authority (NPSA); National Highways as operator.	NIS Regulations 2018, Sch.1. Infrastructure Act 2015 (National Highways licence). Highways Act 1980.
Scotland trunk roads	Scottish Ministers — NIS CA; Transport Scotland (operator)	Scottish Ministers are the NIS CA for road transport in Scotland.	NIS Regulations 2018, Sch.1.
Northern Ireland roads	Department of Finance (NI) — NIS CA; Department for Infrastructure (NI)	As above for NI.	NIS Regulations 2018, Sch.1.
Connected and automated vehicles	DfT; Vehicle Certification Agency; Driver and Vehicle Standards Agency (DVSA)	Vehicle cyber security type-approval (United Nations Economic Commission for Europe (UNECE) R155/R156) and automated vehicle authorisation.	Automated Vehicles Act 2024; UK (NI) Type Approval regime.

10.3 Aviation and space

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
Airports, airlines, air navigation services (NATS), ground handlers and cargo	Department for Transport (DfT) (Secretary of State) and Civil Aviation Authority (CAA), jointly — Network and Information Systems (NIS) Competent Authority (CA); DfT Aviation Security	Cyber: joint NIS CA. CAA's Cyber Security Oversight Team runs the CAP 1753 process (Cyber Assessment Framework (CAF)-based assessment, ASSURE accredited audits, certificate of compliance) across airworthiness, operations, aerodromes, air traffic management (ATM) and aviation security. Physical: the National Aviation Security Programme (NASP) is set by DfT under statute and enforced by the CAA as the aviation security regulator (directions, inspections, security-restricted areas, screening).	NIS Regulations 2018, Sch.1. Aviation Security Act 1982; Aviation and Maritime Security Act 1990; Civil Aviation Act 2012 (transfer of aviation security regulation to CAA); UK retained Regulation (EC) 300/2008 and (EU) 2015/1998.
Spaceports, launch operators, satellite operators and ground segment	CAA (UK spaceflight regulator); Department for Science, Innovation and Technology (DSIT) and UK Space Agency (Lead Government Department (LGD)); Ofcom (spectrum and satellite filings); Ministry of Defence (MOD) / UK Space Command	Cyber and physical: CAA licence conditions require a security regime for spaceflight activities, including cyber security of launch and range systems; UK Space Agency (UKSA)/DSIT lead sector protective security; Ofcom regulates spectrum.	Space Industry Act 2018 and Space Industry Regulations 2021 (Part 8, security); Outer Space Act 1986; Wireless Telegraphy Act 2006.

10.4 Maritime, ports and shipping

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
Ports, harbour authorities, port facilities, vessel traffic services and terminal operators	Department for Transport (DfT) (Secretary of State) — sole Network and Information Systems (NIS) Competent Authority (CA) for water transport and the Maritime Security regulator; Maritime and Coastguard Agency (MCA); Border Force; port police	Cyber: DfT is NIS CA (harbour authorities, port operators and vessel traffic services (VTS) providers designated as Operators of Essential Services (OES)); DfT/Institution of Engineering and Technology (IET) Ports and Port Systems Cyber Security Code of Practice. Physical: DfT Maritime Security approves Port Facility Security Plans and inspects compliance with the International Ship and Port Facility Security (ISPS) Code; MCA regulates ship safety and flag-state matters.	NIS Regulations 2018, Sch.1. Aviation and Maritime Security Act 1990; Ship and Port Facility (Security) Regulations 2004 (retained Regulation (EC) 725/2004 and Directive 2005/65/EC); Port Security Regulations 2009; Merchant Shipping Act 1995.
UK-flagged ships and offshore support vessels	MCA (flag state); DfT Maritime Security; Registrar General of Shipping	Physical: Ship Security Plans under ISPS/Ship and Port Facility (Security) Regulations 2004; MCA MIN 647 and DfT Cyber Security Code of Practice for Ships (International Maritime Organization (IMO) Resolution MSC.428(98) requires cyber risk in Safety Management Systems).	Merchant Shipping Act 1995; International Safety Management (ISM) and ISPS Codes as applied in UK law.
Northern Ireland ports	DfT (maritime security is UK-wide); Department of Finance (NI) for NIS	Maritime security is a reserved matter; DfT acts UK-wide.	As above.

11. Communications and digital infrastructure

Lead Government Department: Department for Science, Innovation and Technology. Ofcom is the statutory regulator across telecoms security, digital infrastructure (under the Network and Information Systems Regulations) and, prospectively, data centres.

11.1 Telecommunications networks and services

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
Public electronic communications networks and services (fixed, mobile, core networks, broadband, 5G, submarine cable landing)	Ofcom — telecoms security regulator; Department for Science, Innovation and Technology (DSIT) — policy and designated vendor powers	Cyber and physical: the Telecommunications (Security) Act 2021 places duties on providers to identify, reduce and prepare for security compromises, including physical protection of network sites, supply-chain and vendor risk, and network access. Ofcom monitors, audits and enforces (fines up to 10% of turnover or £100,000 per day). DSIT issues the Telecommunications Security Code of Practice (Dec 2022; update consulted on in 2025–26) and designated vendor directions (e.g. removal of Huawei equipment).	Communications Act 2003 ss.105A–105Z (inserted by the Telecommunications (Security) Act 2021); Electronic Communications (Security Measures) Regulations 2022; Telecommunications Security Code of Practice. Broadcasting and spectrum: Ofcom under the Wireless Telegraphy Act 2006 and Broadcasting Acts.
Emergency Services Network (ESN) and Airwave	Home Office (owner/customer); Ofcom (spectrum, telecoms security of the underlying provider)	Home Office contractually and through security accreditation; provider regulated by Ofcom under Telecommunications (Security) Act 2021 (TSA).	Home Office ESN programme; Communications Act 2003.

11.2 Subsea cables and undersea infrastructure

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
Submarine telecommunications cables (landing stations, cable routes in UK territorial waters and on the UK Continental Shelf (UKCS))	Ofcom (as part of the provider's Telecommunications (Security) Act 2021 (TSA) network); Department for Science, Innovation and Technology (DSIT) (policy); Ministry of Defence (MOD) / Royal Navy and Joint Maritime Security Centre (JMSC) (protection and maritime domain awareness); National Protective Security Authority (NPSA) and National Cyber Security Centre (NCSC) (advice); Marine Management Organisation / Marine Directorate Scotland (marine licensing); Crown Estate (seabed)	Cyber and physical: today, cable systems operated by public communications providers fall within the TSA 2021 security duties enforced by Ofcom; physical protection at sea relies on the 1885 Act offences, naval presence and JMSC coordination. On 29 May 2026 the government announced new legislation to impose TSA-style security duties on cable owners and operators, tougher criminal offences for vessel owners who intentionally or recklessly damage cables, and emergency powers to direct businesses to protect cables; a white paper is expected later in 2026.	Submarine Telegraph Act 1885 (to be replaced); Communications Act 2003 (TSA 2021); Marine and Coastal Access Act 2009; United Nations Convention on the Law of the Sea (UNCLOS) Articles 21, 58, 79, 113–115 (territorial sea, Exclusive Economic Zone (EEZ) and continental shelf rights). Joint Committee on the National Security Strategy reports (2025–26) on subsea cable resilience.
Subsea power cables and pipelines	Ofgem / Department for Energy Security and Net Zero (DESNZ) (see Section 8); Health and	As per energy regimes; included in the undersea infrastructure protection work.	Pipelines Safety Regulations 1996;

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
	Safety Executive (HSE) (pipelines); MOD/JMSC		Petroleum Act 1998; Energy Act 2004.

11.3 Digital infrastructure, data centres and digital services

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
Digital infrastructure: internet exchange points, DNS service providers, top-level domain registries	Ofcom — Network and Information Systems (NIS) Competent Authority	Cyber: NIS Operators of Essential Services (OES) regime (Cyber Assessment Framework (CAF)-based).	NIS Regulations 2018, Sch.1 (Digital Infrastructure — Office of Communications).
Data centres (colocation and enterprise)	Proposed under the Bill: Department for Science, Innovation and Technology (DSIT) (Secretary of State) as designating authority and Ofcom as operational regulator; DSIT is Lead Government Department (LGD) (data centres designated critical national infrastructure (CNI) on 12 September 2024)	Cyber and (through the code of practice) physical resilience: designation of operators above thresholds (colocation >1 MW; enterprise ≥10 MW rated IT load), incident reporting, inspections and penalties. Currently non-statutory (Data Centre Security and Resilience Code of Practice) pending Royal Assent and commencement.	Cyber Security and Resilience Bill, clause 4 and Schedule (data centres as essential services). Thresholds may be adjusted by regulations.
Relevant digital service providers (cloud computing, online marketplaces, search engines)	Information Commissioner's Office (ICO) / Information Commission — NIS Competent Authority (CA)	Cyber: NIS Relevant Digital Service Provider (RDSP) regime; incident reporting; the Bill extends scope and reporting duties.	NIS Regulations 2018, Sch.1 and Part 4.
Managed service providers and designated critical suppliers	Proposed under the Bill: ICO / Information Commission for relevant managed service providers; the sector CA for critical suppliers designated in an OES supply chain	Cyber: security duties, incident reporting (24/72 hours), enforcement.	Cyber Security and Resilience Bill (relevant managed service providers; designated critical suppliers).
Cloud providers to the financial sector (critical third parties)	Bank of England, Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) (see Section 13)	Operational resilience oversight; first designations (AWS, Google Cloud, Microsoft, Oracle) took effect 13 July 2026.	Financial Services and Markets Act (FSMA) 2000 as amended by FSMA 2023.

12. Water and wastewater networks

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
Water supply and distribution — England	Drinking Water Inspectorate (DWI), acting for the Secretary of State (Department for Environment, Food and Rural Affairs (Defra)) — Network and Information Systems (NIS) Competent Authority (CA); Defra — Lead Government Department (LGD); Ofwat — economic regulator with resilience duty	Cyber: DWI regulates water Operators of Essential Services (OES) under NIS (Cyber Assessment Framework (CAF)-based, incident reporting). Physical: Defra's Security and Emergency Measures Direction (SEMD) 2022 requires water companies to have security and emergency plans, with DWI assessing compliance; National Protective Security Authority (NPSA) advice; Ofwat's resilience duty and price-control security allowances.	NIS Regulations 2018, Sch.1. Water Industry Act 1991 s.208 (SEMD 2022). Water Act 2014 (Ofwat resilience duty). Independent Water Commission (Cunliffe review, 2025) proposed a single integrated regulator for England and Wales — legislation pending.
Water supply — Wales	Welsh Ministers — NIS CA (DWI performs the function); Ofwat	As England.	NIS Regulations 2018, Sch.1; Water Industry Act 1991.
Water supply — Scotland (Scottish Water)	Drinking Water Quality Regulator for Scotland (DWQR) — NIS CA; Scottish Government; Water Industry Commission for Scotland; Scottish Environment Protection Agency (SEPA)	Cyber: DWQR regulates Scottish Water under NIS (DWQR NIS incident reporting guidance, 2024). Physical: Scottish Government with NPSA; Scottish Water security directions.	NIS Regulations 2018, Sch.1. Water Industry (Scotland) Act 2002.
Water supply — Northern Ireland (NI Water)	Department of Finance (NI) — NIS CA; Department for Infrastructure (NI); Utility Regulator	As above for NI.	NIS Regulations 2018, Sch.1. Water and Sewerage Services (NI) Order 2006.
Wastewater and sewerage	Ofwat (economic); Environment Agency / Natural Resources Wales (NRW) / SEPA / Northern Ireland Environment Agency (NIEA) (environment); Defra	Not an OES sector under the NIS Regulations 2018; covered by SEMD and sector resilience oversight. The Bill's powers would allow addition by regulations.	Water Industry Act 1991; Environment Act 2021.

13. Other critical national infrastructure sectors

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
Health (NHS trusts, health boards, ambulance services, health IT suppliers)	Department of Health and Social Care (DHSC) (Secretary of State) — Network and Information Systems (NIS) Competent Authority (CA) for England, with NHS England delivering assurance (Data Security and Protection Toolkit / Cyber Assessment Framework (CAF)-aligned); Welsh Ministers; Scottish Ministers; Department of Finance (NI); Care Quality Commission (safety)	Cyber: NIS Operators of Essential Services (OES) regime for healthcare settings. Physical: NHS England Emergency Preparedness, Resilience and Response (EPRR) framework and DHSC as Lead Government Department (LGD).	NIS Regulations 2018, Sch.1. Health and Care Act 2022. Bill expected to bring health-sector managed service providers into scope.
Finance (banks, payment systems, financial market infrastructure, critical third parties)	Bank of England (financial market infrastructures (FMIs), systemic payment systems); Prudential Regulation Authority; Financial Conduct Authority; HM Treasury — LGD; Payment Systems Regulator	Cyber and operational resilience: rules on operational resilience (important business services, impact tolerances, in force since March 2022 with full compliance from March 2025); CBEST threat-led penetration testing; incident reporting policy statements (March 2026); oversight of designated Critical Third Parties from 13 July 2026. Physical: HM Treasury (HMT)/ Bank with National Protective Security Authority (NPSA) (e.g. cash centres, data centres).	Financial Services and Markets Act (FSMA) 2000 as amended by FSMA 2023 (critical third parties, Part 18); Banking Act 2009 Part 5; Prudential Regulation Authority (PRA) Rulebook and Financial Conduct Authority (FCA) Handbook (SYSC 15A). Finance is outside NIS.
Chemicals (major-hazard chemical manufacturing, storage and pipelines)	Health and Safety Executive (HSE) (with the Environment Agency, Natural Resources Wales (NRW) or Scottish Environment Protection Agency (SEPA) as joint Control of Major Accident Hazards Regulations 2015 (COMAH) Competent Authority); Department for Business and Trade — LGD; Home Office (security of hazardous substances, chemical, biological, radiological and nuclear (CBRN)); Counter Terrorism Policing	Physical/process safety: COMAH safety reports and inspections, including cyber threats to safety-instrumented systems (HSE OG86). Protective security of top-tier sites: NPSA/Counter Terrorism Security Adviser (CTSA) advice and Home Office guidance on precursor and hazardous chemicals.	Control of Major Accident Hazards Regulations 2015; Dangerous Substances and Explosive Atmospheres Regulations 2002; Poisons Act 1972 (as amended 2015).
Emergency services (police, fire and rescue, ambulance, coastguard)	Home Office — LGD (police, fire) with His Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS); DHSC (ambulance); Department for Transport (DfT)/Maritime and Coastguard Agency (MCA) (coastguard); Police Digital Service / National Police Chiefs' Council (NPCC) (cyber)	Cyber: not NIS-designated; national policing cyber assurance via the Police Digital Service and National Cyber Security Centre (NCSC). Physical: Home Office and NPSA.	Civil Contingencies Act 2004 (Category 1 responders); Policing and Crime Act 2017.
Food, farming and fisheries	See Section 5 for the full farm-to-fork treatment.	Department for Environment, Food and Rural Affairs (Defra) — LGD; no statutory security regulator.	Agriculture Act 2020; Fisheries Act 2020; Food Safety Act 1990.
Government (critical government systems and estates)	Cabinet Office (Government Security Group, GovAssure, Government Security Centres); departmental security officers; NCSC	Cyber: GovAssure CAF-based assurance of critical government systems; Government Cyber Security Strategy. Physical: Government Security	Cabinet Office functional standards; Security Policy Framework.

Network / asset class	Regulator(s) / authority	Security remit	Legal basis and notes
		Group and NPSA; Government Functional Standard GovS 007 (Security).	
Defence (defence estates, industry and networks)	Ministry of Defence (Defence Security, Ministry of Defence (MOD) Police, Defence Nuclear Safety Regulator); Defence Cyber Protection Partnership (industry supply chain)	Internal MOD regulation of physical and cyber security, including Defence Standard (DEFSTAN) 05-138 cyber requirements for suppliers.	Official Secrets Acts; MOD Security Policy; Defence and Security Public Contracts Regulations 2011.

14. The offshore dimension: territorial waters, the UK Continental Shelf and the Exclusive Economic Zone

UK security regulation reaches offshore infrastructure through several overlapping mechanisms rather than one offshore security regulator. The territorial sea extends 12 nautical miles from baselines (Territorial Sea Act 1987); beyond it, the UK exercises sovereign rights over the continental shelf (Continental Shelf Act 1964) and the Exclusive Economic Zone (Marine and Coastal Access Act 2009 s.41) for energy production and cables, consistent with the United Nations Convention on the Law of the Sea.

Mechanism	How it applies offshore
Network and Information Systems (NIS) Regulations 2018	Apply to operators of essential services wherever their UK network and information systems are located; offshore production facilities, offshore wind farms and interconnectors operated by designated Operators of Essential Services (OES) are within scope of Department for Energy Security and Net Zero (DESNZ)/Ofgem regulation.
Health and Safety Executive (HSE) Energy Division (offshore)	Regulates the safety of offshore installations (fixed and mobile) and pipelines in UK territorial waters and on the UK Continental Shelf (UKCS), including safety cases, verification schemes and the security of safety-critical control systems. The Offshore Safety Act 1992 and the Offshore Installations (Offshore Safety Directive) (Safety Case) Regulations 2015 apply to 'relevant waters' extending to the continental shelf.
Safety zones	500 m automatic safety zones around oil and gas installations (Petroleum Act 1987 s.21) and safety zones around renewable energy installations (Energy Act 2004 s.95) are criminal-law exclusion zones enforceable by the Royal Navy, police and Border Force.
Office for Nuclear Regulation (ONR) (nuclear transport)	ONR regulates the security of nuclear material carried on UK-flagged vessels anywhere and on any vessel in UK waters (Nuclear Industries Security Regulations 2003 (NISR), Part 3).
Department for Transport (DfT) Maritime Security / Maritime and Coastguard Agency (MCA) / Joint Maritime Security Centre (JMSC)	The International Ship and Port Facility Security (ISPS) regime applies to UK ports and UK-flagged ships; MCA enforces ship security certification. JMSC provides multi-agency maritime domain awareness across UK waters and the Exclusive Economic Zone (EEZ), and coordinates the response to threats to offshore energy and cable infrastructure.
Ministry of Defence / Royal Navy	Protection of undersea infrastructure and the maritime approaches (e.g. Royal Fleet Auxiliary (RFA) Proteus multi-role ocean surveillance ship; NATO Baltic Sentry participation); no regulatory powers over operators but the primary physical-protection capability at sea.
Marine licensing and seabed	Marine Management Organisation (England), Marine Directorate (Scotland), Natural Resources Wales and Department of Agriculture, Environment and Rural Affairs (DAERA) Marine (NI) license offshore works under the Marine and Coastal Access Act 2009 and Marine (Scotland) Act 2010; the Crown Estate and Crown Estate Scotland lease the seabed. Licence and lease conditions can carry security and resilience requirements, and the National Security and Investment (NSI) Act 2021 applies to acquisitions of offshore energy and cable assets.
Fisheries enforcement	The Marine Management Organisation and devolved fisheries administrations, with the Royal Navy Overseas Patrol Squadron and inshore fisheries authorities, enforce the UK fisheries regime under the Fisheries Act 2020 across the territorial sea and EEZ; fishing vessels are regulated for safety by the MCA (Section 5).
Proposed undersea infrastructure legislation	The May 2026 announcement (white paper expected late 2026) would impose statutory security duties on subsea cable owners/operators, replace the Submarine Telegraph Act 1885 offences, and create emergency direction powers — the first dedicated offshore security regime for communications infrastructure.

15. Bibliography

Sources consulted in preparing this guide, listed alphabetically by originating body. All were accessed on 18 September 2026. Statutory references in the body of the document are to legislation.gov.uk unless otherwise stated.

- Agricultural Engineers Association (2026) *The voice of the agricultural and outdoor power equipment sectors*. Available at: <https://aea.uk.com/>
- All-Party Parliamentary Group for Freight and Logistics (2024) *Securing our supply chains: tackling freight crime*. Available at: <https://motortransport.co.uk/industry-news/mps-call-for-government-action-to-tackle-rising-levels-of-freight-crime/24978.article>
- Angling Trust (2026) *Angling Trust and Environment Agency evolve volunteer support for fisheries protection*. Available at: <https://anglingtrust.net/2026/05/06/angling-trust-and-environment-agency-evolve-volunteer-support-for-fisheries-protection-2/>
- Baker Botts (2026) *UK government announces new laws for submarine cable protection*. Available at: <https://www.bakerbotts.com/thought-leadership/publications/2026/june/uk-government-announces-new-laws-for-submarine-cable-protection>
- Bolton Council (n.d.) *Temporary market and car boot guidance*. Available at: <https://www.bolton.gov.uk/downloads/file/990/temporary-market-and-car-boot-guidance>
- Bank of England (2026) *UK financial regulators to begin overseeing Critical Third Parties announced by HM Treasury*. Available at: <https://www.bankofengland.co.uk/news/2026/july/uk-financial-regulators-to-begin-overseeing-critical-third-parties-announced-by-hmt>
- Civil Aviation Authority (2026) *Cyber security oversight (CAP 1753)*. Available at: <https://www.caa.co.uk/commercial-industry/cyber-security/cyber-security-oversight/>
- Civil Aviation Authority (2026) *Known consignor scheme*. Available at: <https://www.caa.co.uk/Commercial-industry/Security/Compliance/Known-consignor-scheme/>
- Clyde & Co (2026) *Carriers, brokers and dealers reform: transition to the 'controlling or transporting' regime*. Available at: <https://www.clydeco.com/en/insights/2026/06/carriers-brokers-and-dealers-reform-transition-to>
- Countryside Alliance (2025) *Gutted ATV theft law fails farmers*. Available at: <https://www.countryside-alliance.org/news-content/type/gutted-atv-theft-law-fails-farmers>
- Construction Equipment Association (2026) *National Construction and Agricultural Theft Team (NCATT)*. Available at: <https://thecea.org.uk/ncatt>
- Combined Industries Theft Solutions (2026) *National Construction and Agricultural Theft Team and CESAR Scheme quarterly reports*. Available at: <https://www.cits.uk.com/ncatt.php>
- Department for Energy Security and Net Zero and Ofgem (2026) *Whole-energy resilience: reshaping cyber regulation in downstream gas and electricity (consultation)*. Available at: <https://assets.publishing.service.gov.uk/media/69c51142471d520038d0f68d/whole-energy-resilience-consultation-document.pdf>
- Department for Energy Security and Net Zero, NCSC, Ofgem and NESO (2026) *Energy sector cyber security strategy*. Available at: <https://www.gov.uk/government/publications/energy-sector-cyber-security-strategy/energy-sector-cyber-security-strategy>
- Department for Environment, Food and Rural Affairs (2026) *Fly-tipping statistics for England, 2024 to 2025*. Available at: <https://www.gov.uk/government/statistics/fly-tipping-statistics-for-england>
- Department for Environment, Food and Rural Affairs (2026) *Waste Crime Action Plan*. Available at: <https://www.gov.uk/government/publications/waste-crime-action-plan/waste-crime-action-plan>
- Department for Environment, Food and Rural Affairs (2024) *United Kingdom Food Security Report 2024*. Available at: <https://www.gov.uk/government/statistics/united-kingdom-food-security-report-2024>
- Department for Science, Innovation and Technology (2024) *The UK Product Security and Telecommunications Infrastructure (Product Security) regime*. Available at: <https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime>

- Department for Science, Innovation and Technology (2025) *Proposals to update the Telecommunications Security Code of Practice 2022*. Available at: <https://www.gov.uk/government/consultations/proposals-to-update-the-telecommunications-security-code-of-practice-2022/proposals-to-update-the-telecommunications-security-code-of-practice-2022-what-we-are-consulting-on>
- Department for Science, Innovation and Technology (2026) *Second post-implementation review of the Network and Information Systems Regulations 2018*. Available at: <https://www.gov.uk/government/publications/second-post-implementation-review-of-the-network-and-information-systems-regulations-2018/second-post-implementation-review-of-the-network-and-information-systems-regulations-2018>
- Department for Transport (2020) *Implementation of the NIS Directive: DfT guidance*. Available at: <https://assets.publishing.service.gov.uk/media/5ee3a21ae90e0704315ecf32/implementation-of-the-nis-directive-dft-guidance-document.pdf>
- Department for Transport (2020) *Rail cyber security: guidance to industry*. Available at: <https://assets.publishing.service.gov.uk/media/5efcace9e90e075c52d05a94/rail-cyber-security-guidance-to-industry-document.pdf>
- Department for Transport (2023) *Code of practice: cyber security for ships*. Available at: <https://assets.publishing.service.gov.uk/media/64c929c0d8b1a71bd8b05e80/code-of-practice-cyber-security-for-ships.pdf>
- Department for Transport (2024) *Ports and port systems: cyber security code of practice*. Available at: <https://gov.uk/government/publications/ports-and-port-systems-cyber-security-code-of-practice>
- Department of Finance (Northern Ireland) (2026) *NIS contacts and useful links*. Available at: <https://www.finance-ni.gov.uk/articles/nis-contacts-useful-links>
- Drinking Water Quality Regulator for Scotland (2024) *Guidance for Scottish Water on NIS incident reporting*. Available at: <https://dwqr.scot/media/etqj0juy/dwqr-nis-guidance-for-scottish-water-on-nis-incident-reporting-may-2024-v2-0.pdf>
- Environment Agency (2026) *Joint Unit for Waste Crime (JUWC): end of year report 2025 to 2026*. Available at: <https://www.gov.uk/government/publications/joint-unit-for-waste-crime-juwc-end-of-year-report-2025-to-2026/joint-unit-for-waste-crime-juwc-end-of-year-report-2025-to-2026>
- Environment, Food and Rural Affairs Committee (2025) *Biosecurity at the border: Britain's illegal meat crisis (HC 1296)*. Available at: <https://publications.parliament.uk/pa/cm5901/cmselect/cmenvfru/1296/report.html>
- European Commission (2026) *Cyber Resilience Act (Regulation (EU) 2024/2847)*. Available at: <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>
- Food Standards Agency (2025) *National Food Crime Unit: annual update*. Available at: <https://www.gov.uk/government/publications/fsa-25-12-06-national-food-crime-unit-annual-update/national-food-crime-unit-annual-update>
- Fleet News (2026) *Nine thefts a day from trucks in 2025 (NaVCIS annual figures)*. Available at: <https://www.fleetnews.co.uk/news/nine-thefts-a-day-from-trucks-in-2025>
- Forestry Commission (2024) *How we're using the power of the courts to clamp down on illegal felling*. Available at: <https://forestrycommission.blog.gov.uk/2024/02/13/how-were-using-the-power-of-the-courts-to-clamp-down-on-illegal-felling/>
- Gowling WLG (2026) *Regulating data centres: the Cyber Security and Resilience Bill*. Available at: <https://gowlingwlg.com/en/insights-resources/articles/2026/regulating-data-centres-the-cyber-security-and-resilience-bill>
- Health and Safety Executive (n.d.) *Cyber security: electrical, control and instrumentation*. Available at: <https://www.hse.gov.uk/eci/cyber-security.htm>
- Health and Safety Executive (n.d.) *COMAH: information and guidance*. Available at: <https://www.hse.gov.uk/comah/guidance.htm>
- Historic England (2024) *Extent of heritage and cultural property crime in England revealed*. Available at: <https://historicengland.org.uk/whats-new/news/heritage-crime-research-findings-revealed/>
- Historic England (n.d.) *Heritage crime*. Available at: <https://historicengland.org.uk/advice/caring-for-heritage/heritage-crime/>

- Home Office (2022) *Scrap Metal Dealers Act 2013: post implementation review*. Available at: https://assets.publishing.service.gov.uk/media/62448ae9d3bf7f32add7825f/Annex_A_20220114_Scrap_Metal_Dealers_PIR_FINAL_FOR_PUBLICATION.pdf
- Home Office (2026) *Record funding to protect faith communities*. Available at: <https://www.gov.uk/government/news/places-of-worship-scheme-provides-record-levels-of-funding>
- Home Office (2026) *Crime and Policing Act 2026: overarching factsheet*. Available at: <https://www.gov.uk/government/publications/crime-and-policing-act-2026-factsheets/crime-and-policing-act-overarching-factsheet>
- Home Office (2026) *Terrorism (Protection of Premises) Act 2025: statutory guidance (April 2026)*. Available at: https://assets.publishing.service.gov.uk/media/69d7c1ff4abe5b6c5ddf26c9/Web_accessible_PDF_-_Terrorism_Protection_of_Premises_Act_2025_Stat_Guidance.pdf
- Home Office (2026) *Understanding Martyn's Law and the SIA's role as regulator*. Available at: <https://www.gov.uk/guidance/understanding-martyns-law-and-the-sias-role-as-regulator>
- House of Commons Library (2026) *Cyber Security and Resilience (Network and Information Systems) Bill 2024-26 (CBP-10442)*. Available at: <https://commonslibrary.parliament.uk/research-briefings/cbp-10442/>
- House of Lords Library (2026) *Cyber Security and Resilience (Network and Information Systems) Bill (LLN-2026-0032)*. Available at: [https://researchbriefings.files.parliament.uk/documents/LLN-2026-0032/2026-0032-Cyber-Security-and-Resilience-\(Network-and-Information-Systems\)-Bill-LARGE.pdf](https://researchbriefings.files.parliament.uk/documents/LLN-2026-0032/2026-0032-Cyber-Security-and-Resilience-(Network-and-Information-Systems)-Bill-LARGE.pdf)
- Joint Committee on the National Security Strategy (2025) *Subsea telecommunications cables: resilience and crisis preparedness — government response*. Available at: <https://publications.parliament.uk/pa/jt5901/jtselect/jtnatsec/1574/report.html>
- National Audit Office (2026) *Resilience of the food supply chain to disruptions*. Available at: <https://www.nao.org.uk/wp-content/uploads/2026/09/Resilience-of-the-food-supply-chain-to-disruptions.pdf>
- Northern Ireland Audit Office (2025) *Waste crime in Northern Ireland*. Available at: <https://www.niauditoffice.gov.uk/publications/html-document/waste-crime-northern-ireland>
- National Business Crime Centre (2026) *National Vehicle Crime Reduction Partnership*. Available at: <https://nbcc.police.uk/partnerships/partners/national-vehicle-crime-reduction-partnership-nvcrp>
- National Vehicle Crime Intelligence Service (2026) *NaVCIS Freight*. Available at: <https://navcis.police.uk/freight/>
- National Farmers' Union (2026) *NFU Mutual Rural Crime Report reveals cost of rural crime has fallen*. Available at: <https://www.nfuonline.com/news/nfu-mutual-rural-crime-report/>
- National Cyber Security Centre and National Farmers' Union (2023) *Cyber security for farmers: practical tips on how to stay safe*. Available at: https://www.ncsc.gov.uk/files/NCSC_Cyber%20Security%20Guide%20for%20Farmers-%20digital.pdf
- National Police Chiefs' Council (2025) *Crackdown on organised crime gangs targeting Britain's farms and countryside (Rural and Wildlife Crime Strategy 2025–2028)*. Available at: <https://news.npcc.police.uk/releases/crackdown-on-organised-crime-gangs-targeting-britains-farms-and-countryside>
- Norfolk Constabulary (2026) *New livestock worrying law comes into force*. Available at: <https://www.norfolk.police.uk/news/norfolk/news/news/2026/march/new-livestock-worrying-law-comes-into-force/>
- National Protective Security Authority (2026) *Critical National Infrastructure: frequently asked questions*. Available at: <https://www.npsa.gov.uk/frequently-asked-questions-0>
- Office for Nuclear Regulation (2026) *Civil nuclear security*. Available at: <https://www.onr.org.uk/our-work/what-we-regulate/civil-nuclear-security>
- Ofgem (2021) *NIS Directive and NIS Regulations 2018: Ofgem guidance for Operators of Essential Services*. Available at: <https://www.ofgem.gov.uk/publications-and-updates/nis-directive-and-nis-regulations-2018-ofgem-guidance-operators-essential-services>
- Road Haulage Association (2024) *Driving down freight crime: RHA's call to police and crime commissioners*. Available at: https://www.rha.uk.net/Portals/0/Media%20Center/RHA_Driving%20Down%20Freight%20Crime_Manifesto.pdf

- Sentencing Council (2026) *Hare coursing: sentencing guideline*. Available at: <https://sentencingcouncil.org.uk/guidelines/hare-coursing>
- Safeguard Systems (2025) *Is solar farm crime on the rise? Trends and data*. Available at: <https://safeguardsystems.co.uk/solar-farm-crime/is-solar-farm-crime-on-the-rise-trends-and-data/>
- Scottish Government (2026) *Market operators licence (Scotland)*. Available at: <https://www.gov.uk/market-operators-licence-scotland>
- Scottish Government (2026) *Litter and flytipping*. Available at: <https://www.gov.scot/policies/managing-waste/litter-and-flytipping/>
- Transported Asset Protection Association EMEA (2026) *TAPA EMEA intelligence service*. Available at: <https://tapaemea.org/incident-service/>
- TT Club (2025) *TT Club calls for urgent overhaul of lorry parking security across the UK to combat rising cargo theft*. Available at: <https://www.ttclub.com/news-and-resources/news/article/tt-club-calls-for-urgent-overhaul-of-lorry-parking-security-across-the-uk-to-combat-rising-cargo-theft/>
- UK Parliament (2025) *Dogs (Protection of Livestock) (Amendment) Act 2025*. Available at: <https://www.legislation.gov.uk/ukpga/2025/32>
- UK Parliament (2013) *Scrap Metal Dealers Act 2013*. Available at: <https://www.legislation.gov.uk/ukpga/2013/10>
- UK Parliament (2018) *The Network and Information Systems Regulations 2018 (SI 2018/506), Schedule 1*. Available at: <https://www.legislation.gov.uk/uksi/2018/506/schedule/1>
- UK Parliament (2021) *Telecommunications (Security) Act 2021*. Available at: <https://www.legislation.gov.uk/ukpga/2021/31>
- UK Parliament (2026) *Crime and Policing Act 2026*. Available at: <https://www.legislation.gov.uk/ukpga/2026/20/contents/enacted>
- UK Parliament (2026) *Freight Crime Bill: bill page*. Available at: <https://bills.parliament.uk/bills/3950>
- UK Parliament (2026) *Cyber Security and Resilience (Network and Information Systems) Bill: bill page*. Available at: <https://bills.parliament.uk/bills/4035>



OUR MISSION

“The UK’s national programme to stop rural crime before it starts — for farmers, estates, insurers and retailers alike.”

Rural SafeGuard is the UK’s first, commercially available, national programme designed to reduce rural crime before it happens — helping to protect livelihoods, strengthen food security, and make the countryside safer for all.

OUR PURPOSE

Rural SafeGuard exists to introduce farmers, landowners, insurers and rural communities to the security sector, and to share the best practices already on offer to other industrial sectors — building safer rural communities, together.

GET IN TOUCH

Frank Cannon CSyP, Founding Director, Rural SafeGuard Crime Reduction Programme

frank.cannon@ruralsafeguard.com

07742 569943

RURAL SAFEGUARD

ruralsafeguard.com

OPTIMAL RISK GROUP

optimalrisk.com

