Critical National Infrastructure

Last Updated: 23 June 2025

Critical National Infrastructure

Critical National Infrastructure (CNI) are those critical elements of infrastructure whose loss or compromise could severely impact the delivery of essential services or have significant impact on national security, national defence, or the functioning of the state. It also includes some functions, sites and organisations which are not critical to the maintenance of essential services, but which need protection due to the potential danger to the public (civil nuclear and chemical sites, for example).

The 13 CNI sectors

In the UK, there are 13 CNI sectors:

- Chemicals
- Civil Nuclear
- Communications
- Defence
- Emergency Services
- Energy
- Finance
- Food
- Government
- Health
- Space
- Transport
- Water

Several sectors have defined 'sub-sectors'; Emergency Services for example is split into Police, Ambulance, Fire and Rescue Services and Coast Guard. In September 2024, Data Infrastructure was formally designated as a sub-sector of Communications, alongside Telecommunications and Internet, Post and Broadcast.

Each sector is overseen by a relevant Lead Government Department (LGD), that is responsible for sectoral policy, guidance and engagement with industry.

'Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:

a) Major detrimental impact on the availability, integrity or delivery of essential services - including those services whose integrity, if compromised, could result in significant loss of life or casualties - taking into account significant economic or social impacts; and/or

b) Significant impact on national security, national defence, or the functioning of the state.'

NPSA is focussed on providing advice and assistance to those who have responsibility for protecting these most crucial elements of the UK's national infrastructure from national security threats.

Criticalities Process

Improving our understanding of Critical National Infrastructure

The UK's Critical National Infrastructure (CNI) is increasingly interconnected and interdependent, making it harder for government to understand and manage the risk faced by the UK. Government has developed a new methodology to collect this data – the Criticalities Process – and is building a new tool to visualise and interrogate the data produced – the CNI Knowledge Base.

The opportunity for the UK

An accurate, shared understanding of the most critical infrastructure in the UK will enable government to better understand and better manage the risk faced by our CNI. Our world-leading approach will provide the UK with the tools it needs to take data-driven decisions to improve our resilience and protect our citizens' way of life now and in the future.

The Criticalities Process

Gives risk owners in government (i.e. each sector's Lead Government Department) a common approach to collect and structure data on the CNI they are responsible for. The process supports the systematic identification of the Essential Functions, the Systems that provide them (and their interdependencies), and the Organisations that operate those systems. This information is tied to the impacts that a system's failure would have (both within and across sectors).

The CNI Knowledge Base

The CNI Knowledge Base is the 'Single Source of Truth' for UK CNI, enabling government analysts to visualise the Criticalities data. This software lets risk owners view UK CNI on a map or as a network graph, with interdependencies mapped across it. The tool and data are held in a secure environment, accessed only by appropriately cleared government officials.

CNI Knowledge Base

- Step 1 Map Essential Functions Understanding what is important
- Step 2 Determine Systems Mapping the Systems that provide the function
- Step 3 Assess Sector impacts Understanding the impact of System compromise
- Step 4 Identify supporting Systems, Organisations and Relationships Mapping the Systems in more detail
- Step 5 Assess Cross-sector impacts Understanding the impact on other sectors

How this helps

Supporting government in this work means you are helping protect the functions that everyone in the UK relies on every day to live and to work. This work will also help us help you:

- We can provide you with targeted, practical advice on the most critical technologies and products within the CNI
- We will be able to make better-informed risk management decisions, taking into account the cost and benefit of potential policies
- We will help equip you with better evidence to catalyse change within your organisations, including at board level

Cyber

Responsibility for the protection of the CNI IT networks, data and systems from cyber attack sits with the National Cyber Security Centre (NCSC). NPSA works in partnership with the NCSC so that collectively we deliver holistic advice that takes into account all aspects of protective security.

Related Pages