Cabinet Office

Public Summary of Sector Security and Resilience Plans

2018

Produced by:

Cabinet Office
35 Great Smith Street
LONDON
SW1P 3BQ

www.gov.uk/government/organisations/cabinet-office

Contact:

Civil Contingencies Secretariat
infrastructure@cabinet-office.x.gsi.gov.uk

Publication date: February 2019

Contents

Introduction

Securing the UK's most essential public and private sector services against wide-ranging threats and hazards form an integral part of HMG's National Security Strategy.[1]

The Cabinet Office commissions Lead Government Departments (LGDs) responsible for the UK's 13 critical sectors to produce annual Sector Security and Resilience Plans (SSRPs), which describe:

- LGDs' approaches to critical sector security and resilience;
- their assessments of significant risks to their sectors;
- their approach to security and resilience in the UK; and
- activities they plan to undertake to mitigate and respond to those risks.

The SSRPs are produced by officials in the LGDs, in consultation with infrastructure owners and operators, regulators and government agencies, before being signed-off by ministers.

The genesis of the SSRPs can be found in a report produced by Sir Michael Pitt, 'Learning Lessons from the 2007 Floods'.[2]

The Sector Resilience Plans (SRPs) were originally intended to focus on resilience to flooding. In 2015 the scope of the Plans was expanded to cover all hazards and security threats relevant to each sector and they were renamed 'Sector *Security* and Resilience Plans (SSRPs)'. Henceforth, the SSRPs have included information on physical, personnel and cyber security as well resilience to hazards.

The full SSRPs are classified documents as they contain sensitive security information. However each year, Government publishes unclassified summaries of the Sector Security and Resilience Plans to provide members of the public with information on activity being undertaken in each sector to improve security and resilience.

This document sets out the public summaries of the 2018-19 SSRPs with the intention of promoting public understanding of the risks to the UK's critical sectors and measures being taken by HM Government to mitigate those risks.

To provide some context for the reader, this document also describes:

- what we mean by 'Critical National Infrastructure' and 'critical sectors';
- significant threats and hazards that can affect our critical sectors;
- our approach to security and resilience in the UK; and
- responsibilities of different organisations for critical sectors' security and resilience.

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf

[2] http://webarchive.nationalarchives.gov.uk/20100702222706/http://archive.cabinetoffice.gov.uk/pittreview/_/media/assets/www.cabinetoffice.gov.uk/flooding_review/pitt_review_full%20pdf.pdf

Critical National Infrastructure

National Infrastructure consists of those facilities, systems, sites, information, people, networks and processes necessary for a country to function and upon which daily life depends. 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 dangers they could pose to the public in the event of an emergency (civil nuclear and chemicals sites, for example).

There are some parts of the National Infrastructure system that are judged to be critical to the functioning of the country. This Critical National Infrastructure (CNI) includes buildings, networks and other systems that are needed to keep the UK running and provide the essential services upon which we rely (e.g. energy, finance, telecoms and water services). It also includes infrastructure which, if disrupted, could have a significant impact on our national security, national defence, or the functioning of the state. A significant proportion of our CNI is privately owned.

The UK's Critical Infrastructure is defined by the Government as:

'Those critical elements of Infrastructure (facilities, systems, sites, property, information, people, networks and processes), the loss or compromise of which would result in major detrimental impact on the availability, delivery or integrity of essential services, leading to severe economic or social consequences or to loss of life.'

In the UK, there 13 Critical National Infrastructure Sectors:

Chemicals, Civil Nuclear, Communications, Defence, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport and Water.

Several sectors also have defined 'sub-sectors'; Emergency Services for example can be split into Police, Ambulance, Fire and Rescue Services, and Her Majesty's Coastguard.

Threats and Hazards

The Government's assessment of threats and hazards to CNI is based on a continuous cycle of learning lessons from real world events, drawing on evidence and improving the ways in which we calculate the likelihood and potential impacts (consequences) of threats and hazards.

Understanding the range of threats and hazards facing our CNI is crucial to ensuring security measures and mitigations are proportionate, effective and responsive. The UK's CNI faces various threats and hazards.

Threats

National Infrastructure could be targeted by hostile states, cyber criminals, terrorists or criminals for the purposes of disruption, espionage and/or financial gain.

For example, the Centre for the Protection of National Infrastructure (CPNI) judges that National Infrastructure sectors represent core strategic interests for foreign intelligence services, whose targeting against the sectors is likely to include espionage for economic, political, military or commercial gain.

While the current terrorist threat to the National Infrastructure can be characterised as generally limited and often aspirational, the transport sector continues to face enduringly high levels of threat from international terrorism. In addition, the Emergency Services and Defence sectors (specifically police and military personnel), also face a high level of threat from both international terrorism and Dissident Republic groups in Northern Ireland. With the continual diversification of the threat, the ambition and capability of terrorist groups to target UK Infrastructure is likely to continue to evolve.[3]

The National Cyber Security Centre (NCSC) judges there is also a growing cyber threat. There are now more devices connected to the internet than ever before, and with the growth of our dependence on technology comes increased risk. We know there are hostile states and cyber criminals that may seek to exploit UK organisations and Infrastructure to further their own agenda and prosperity. Campaigns can be persistent, including espionage, intellectual property theft or extortion by ransoming data, or through malware. [4]

Hazards

There are various natural hazards (e.g. flooding, severe weather and storms) that can also disrupt the day-to-day functioning of the UK's National Infrastructure. Disruption to National Infrastructure can also be caused by public disorder and societal pressures such as staff absence – due, for example, to widespread influenza or industrial action - leading to temporary closures, reduced services, or services continuing but at reduced capacity.

With the continual diversification and evolution of threats and hazards, it's important to build the capability of the UK's Infrastructure to withstand and recover from a range of possible events.

[3] https://www.cpni.gov.uk/national-security-threats

[4] https://www.ncsc.gov.uk/news/2018-annual-review

Our Security & Resilience Approach

Government's core objective includes reducing CNI's vulnerability to threats and hazards and improving resilience by strengthening the ability of CNI to withstand and recover from disruption. Its approach to security and resilience focuses on Resistance, Reliability, Redundancy, and Response & Recovery.

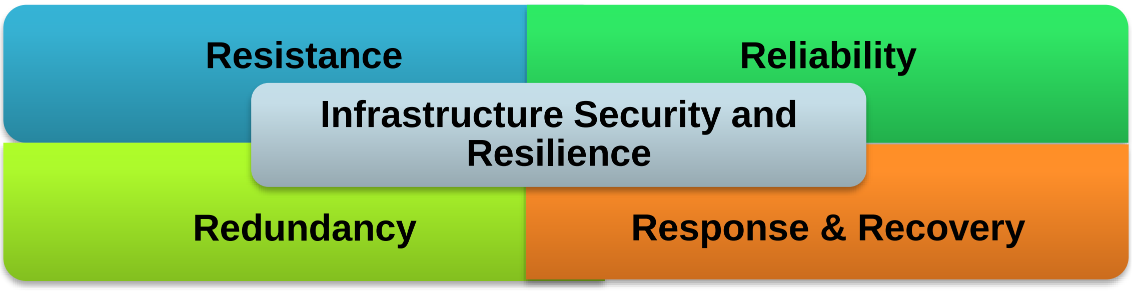

Figure 1: The components of Infrastructure resilience

- **Resistance:** Concerns direct physical protection (e.g. the erection of flood defences). Resistance is ensured by preventing damage or disruption through the protection of Infrastructure against threats and hazards. This includes reducing vulnerability through physical, personnel and cyber security measures.

- **Reliability:** The capability of Infrastructure to maintain operations under a range of conditions to mitigate against damage from an event (e.g. by ensuring that electrical cabling is able to operate in extremes of heat and cold).

- **Redundancy:** The adaptability of an asset or network to ensure the availability of backup installations, systems or processes or spare capacity (e.g. back-up data centres).

- **Response & Recovery:** An organisation's ability to rapidly and effectively respond to, and recover from, disruptive events.

Roles and Responsibilities

A wide range of organisations are responsible for critical sectors' security and resilience, including the owners and operators, emergency services and local and central government.

Infrastructure owners and operators

Day-to-day operating of our National Infrastructure is the responsibility of the owners and operators. They carry out risk assessments at the asset level and make calculated decisions on maintenance, training and investment to improve organisational and asset-level security and resilience.

Regulators

Regulators support Lead Government Departments by ensuring relevant legislation and regulation are observed, for example as part of sites' licence conditions. To build resilience, some regulators can intervene and require organisations to meet particular security and resilience obligations or standards as conditions for their continued operation.

Local authorities and emergency services

In accordance with the Civil Contingencies Act 2004, local authorities and emergency services are required to identify and assess the likelihood and impact of potential emergencies (including Infrastructure emergencies) that could affect members of the public within their areas of jurisdiction. They are also required to develop emergency response plans to address those risks.

Government Agencies

Several agencies provide central government, regulators and Infrastructure owners and operators with advice on Infrastructure risks and mitigation. For example, the Centre for the Protection of National Infrastructure (CPNI) provides protective security advice to businesses and organisations across the UK's National Infrastructure. They also provide integrated advice on physical and personnel security, aimed at minimising risk and reducing our vulnerability to terrorism, espionage, and other national security threats.

The National Cyber Security Centre (NCSC) was established in 2016 as part of the Government Communications Headquarters (GCHQ) and brings together cyber expertise from a wide range of previously disparate cyber organisations. The Centre's main purpose is to reduce the cyber security risk to the UK, working with businesses and individuals to provide authoritative and coherent cyber security advice and cyber incident management, underpinned by world class research and innovation.

Lead Government Departments

Lead Government Departments are responsible for sector-level security and resilience policy development (including legislation). They produce the Sector Security and Resilience Plans (SSRPs), which set out each Department's understanding of the risks to their sectors and the key activities they will undertake to address those risks during the year ahead. The 2018-19 SSRPs are summarised in the following section of this document.

Public Summaries

This section of the document sets out the public summaries of the 2018-19 Sector Security and Resilience Plans (SSRPs). The table below shows which Lead Government Department is responsible for producing each SSRP.

Sector	Sector Resilience Lead [5]
Chemicals	Department for Business, Energy and Industrial Strategy
Civil Nuclear	Department for Business, Energy and Industrial Strategy
Communications	Department for Digital, Culture, Media and Sport Department for Business, Energy and Industrial Strategy
Defence	Ministry of Defence
Emergency Services	Department of Health and Social Care
	Department for Transport
	Home Office
Energy	Department for Business, Energy and Industrial Strategy
Finance	HM Treasury
Food	Department for Environment, Food and Rural Affairs
Government	Cabinet Office
Health	Department of Health and Social Care
Space	UK Space Agency
Transport	Department for Transport
Water	Department for Environment, Food and Rural Affairs

[5] Where responsibility for the resilience of the sector sits with a Devolved Administration, relevant government departments and the Devolved Administrations worked together to ensure the 2018-19 Sector Security and Resilience Plans covered the entirety of the UK.

Chemicals Sector

Department for Business, Energy and Industrial Strategy

The chemicals sector complies with stringent safety and environmental legislation. Internationally agreed conventions promote the resilience of the sector's infrastructure to the most relevant risks. Work continues to identify and review the resilience of key manufacturing sites to a range of disruptive challenges, in order to complement existing measures to prevent casualties from chemical releases.

Assessment of Existing Resilience

Resilience in the chemical sector is not specifically mandated by regulation, but the requirement for site owners to comply with safety and environmental legislation or conventions promotes a strong safety culture; for example:

- Sites subject to COMAH (Control of Major Accident Hazard) regulations must take all necessary measures to prevent major accidents involving dangerous substances and limit the consequences to people and the environment of any major accidents which do occur, e.g. by working with local emergency planners and responders to prepare suitable emergency plans;
- To support site protection and incident response at the local level, emergency planning authorities work with infrastructure owners to maintain emergency plans and lists of hazardous substances on site.
- The relevant sector trade association requires its members to adopt additional measures, going beyond statutory requirements, which enhance resilience.

Building Resilience

Building resilience in the sector is focused on preventing or minimising casualties following a chemical release. Work continues with stakeholders – site owners, sector organisations and across government – to encourage and promote resilience.

Work will continue to encourage key manufacturing sites to consider their resilience to major risks and to develop mitigating measures so that any impacts on the public will be minimised.

For sites which hold defined quantities of very highly hazardous substances, COMAH safety reports must include details of the measures taken to prevent releases in a variety of scenarios, such as during floods and storms.

Civil Nuclear Sector

Department for Business, Energy and Industrial Strategy

The nuclear sector's resilience to major risks is ensured through high build standards, a stringent regulatory regime, and effective governance.

Assessment of Existing Resilience

The latest annual Nuclear Chief Inspector's Report from the independent nuclear regulator, the Office for Nuclear Regulation, concluded that the UK's civil nuclear sector meets the safety and security standards required to operate. Working with the responsible government department, the Office for Nuclear Regulation, and the Civil Nuclear Constabulary, the sector has adopted an all-risks approach to the safety and security of sites. The civil nuclear industry is required to comply with the following national standards:

Safety: UK nuclear sites have a legal responsibility for ensuring nuclear safety on their sites and are held to account by a robust licensing system.

Security: All UK nuclear sites have an up-to-date approved Nuclear Site Security Plan and meet the standards of security required by the regulator.

Safeguards: The UK's obligations concerning the reporting and/or publication of safeguards related information must be met. Euratom[6] and IAEA[7] reporting on verification activities in respect of civil nuclear material in the UK continues to conclude that there has been no diversion of civil nuclear material from peaceful use in the UK.

Building Resilience

The Department for Business, Energy and Industrial Strategy has worked with partners in Government, the regulator and industry to create a National Framework which establishes a national strategy for UK Nuclear site emergency planning and response.

This National Framework:

- Coordinates all partners involved in this work across the UK;
- Ensures high quality, well-tested emergency response and recovery plans for existing and new build sites; and
- Ensures effective communications with local, national, and international audiences.

[6] European Atomic Energy Committee

[7] International Atomic Energy Agency

Communications Sector

Department for Digital, Culture, Media and Sport
Department for Business, Energy and Industrial Strategy

The communications sector comprises telecommunications, internet, broadcast and postal services. The sector has invested proportionately in its resilience to risks. Like many other sectors, it is vulnerable to prolonged and widespread disruption to services such as fuel and energy, however levels of resilience are good and there are inevitable limits to how far vulnerability to very severe events can be reduced.

Assessment of Existing Resilience

Major risks to the sector include disruption to energy and fuel as well as damage to key elements of national infrastructure.

Resilience-building is driven by a combination of competitive pressures, new technologies and the need to meet legislative requirements, licences or standards.

Resilience measures include back-up power generation, service prioritisation and the take up of advice to protect key sites and networks from natural hazards as well as physical and electronic security threats.

The sector has invested proportionately in its resilience. Like many other sectors, it is vulnerable to prolonged and widespread disruption to services such as fuel and energy, however levels of resilience are generally good and industry has contingency plans in place to handle a wide range of risks.

Building Resilience

The sector continues to strengthen relationships with Government, other agencies and industry through joint committees and working groups such as the industry-run Electronic Communications Resilience and Response Group for telecoms/internet and broadcast sub sectors. More specific priorities include:

Telecoms & Internet; Broadcast
To work with industry to assess the risk posed to the sector by cyber-attack and prolonged power loss.

Postal Services
To work with Royal Mail to maintain robust contingency and resilience plans in response to key risks to the national network.

Defence Sector

Ministry of Defence

Defence officially became a sector in 2014, having previously been part of the government sector. Ministry Of Defence (MOD) is responsible for sites that house Critical National Infrastructure. MOD may also be called upon to provide support to the other critical sectors at times of emergency or significant disruption.

Assessment of Existing Resilience

- Defence protects the national security and independence of the UK, operating from a wide variety of sites and using a wide variety of capabilities and equipment. Defence has a number of dependencies, including power supplies, telecoms and key personnel.
- The current assessment of the sector is wide-ranging. It goes beyond the sector's CNI assets, and includes vulnerabilities to threats and hazards, including cyber risks.
- Defence promotes a robust security culture, compliant with HMG Security Framework and working with other departments to maximise the security of our sites, personnel and equipment
- MOD has sites across the UK and has to manage vulnerabilities to all weather and environmental hazards.
- MOD's business continuity policy is in line with the Government Security Framework, which mandates business continuity management systems consistent with the British Standard 22301. This ensures that business units can maintain critical functions despite disruptive events.

Building Resilience

- The 2015 Strategic Defence and Security Review reinforced MOD's role in supporting UK resilience during emergencies.
- Head Office will continue to fulfill a coordinating function, to support top-level budget holders - who understand their business and critical functions best – to understand their resilience requirements.
- MOD is actively addressing physical resilience requirements as part of broader infrastructure improvements driven by a Strategy for Defence Infrastructure.

Emergency Services Sector

Home Office, Department for Transport, Department for Health and Social Care

The emergency services sector is made up of the Police, Ambulance, Fire and Rescue, and HM Coastguard. Compliance with civil protection legislation, the interconnected nature of its networks, well-tested mutual aid agreements, and the geographic spread of services across the UK affords the emergency services sector a considerable degree of resilience

Assessment of Existing Resilience

Emergency Services are subject to the full set of civil protection duties under the Civil Contingencies Act (2004). This includes the requirement to assess the risks and put in place emergency and business continuity plans.

The major risks to the sector are loss of communications and loss of power. The sector is particularly dependent on communications. However, operational effectiveness in times of disruption is managed by the use of a range of satellite and radio communications, as well as local solutions. To support emergency response during periods of disruption from major risks, each service has:

- well tested fall-back arrangements, including back-up operation centres and back-up power supplies;
- the ability to divert emergency calls between call centres;
- inter-service mutual aid agreements underpinned by: compatible communications and control rooms; multi-agency plans, training and exercising; and shared understanding of operational procedures.

Building Resilience

The emergency services continue to work together to improve resilience, including through:

- The Joint Emergency Services Interoperability Principles (JESIP) which aim to improve joint working between Police, Fire & Rescue and Ambulance services when responding to any multi-agency incidents. JESIP is becoming increasingly embedded into the emergency services' business as usual practice, including the integration of JESIP models into local doctrine to achieve a culture of interoperable working.

- The Emergency Services Mobile Communications Programme which is continuing its work to ensure that Airwave's replacement, the Emergency Services Network, delivers an enhanced level of service availability and resilience.

Energy Sector

Department for Business, Energy and Industrial Strategy

The energy supply sector is made up of upstream oil and gas, downstream oil and gas, and electricity. Although infrastructure types and business environments differ, each sub-sector has invested proportionately to build resilience to major risks.

Assessment of Existing Resilience

Major risks to the energy sector include storms and gales, flooding, accidents, and loss of key staff. It is not cost effective or feasible to mitigate every risk, and Government, regulators and the supply industry work together to ensure risks to supply are appropriately mitigated. To build resilience to these and other risks, energy companies:

Adopt an all risks approach: under the Utilities Act 2002, Ofgem introduced performance levels for the gas and electricity industry including supply restoration timescales; and Ofgem's 'RIIO' performance standard for network companies' price control periods, to ensure efficient investment for continued safe and reliable services.

Address specific vulnerabilities, based on regular risk assessments and reviews of resilience problems that have occurred in the UK and elsewhere: for example, companies have been implementing a large programme of flood protection measures over recent years, which is due for completion by the early 2020s.

Put in place contingency arrangements: energy companies have worked extensively to put in place contingency plans in the event of disruption due to severe weather related events and to manage staffing in the event of pandemic flu and other risks.

Building Resilience

- Electricity: Ensuring an acceptable and affordable of level of Black Start service. Black Start is the term given to the restoration plans developed by National Grid to restore the National Electricity Transmission System in the event of its total failure.
- Energy Networks: Assessment of the risk posed by cyber attack.
- Downstream oil: working on maintaining capability to make fuel deliveries in the event of a serious disruption.
- Energy Sector Flood Resilience: Continuing assessment of flood risks to energy assets and flood protection enhancement programmes.

Finance Sector

Her Majesty's Treasury

The UK is one of the most important centres for financial services in the world. Key elements of the global financial system are based in the UK, and the financial firms and infrastructure are key contributors to the economy, providing essential services to citizens, businesses and the government.

Assessment of Existing Resilience

HM Treasury works jointly with the Bank of England, the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA) (collectively the 'Financial Authorities') to assess and manage operational risks to the sector and respond to operational incidents. Risks to the finance sector include the potential disruption caused by cyber-attacks, IT failures, personnel and physical security risks. There is also a potential impact on the finance sector from disruption to other sectors such as energy and telecommunications.

Over the past year, the finance sector has continued to make good progress in improving its resilience to a range of threats and hazards, reflecting the mature approach to resilience and ongoing investment by firms. A significant number of firms have undergone bespoke intelligence-led penetration testing of cyber resilience known as CBEST and have acted to remediate the issues identified. Our incident response frameworks have also been tested and refined.

Building Resilience

Over the next year, the Financial Authorities will deliver a comprehensive work programme to improve the resilience of the finance sector. We will ensure that we have the tools to deliver improved resilience, including drawing on the expertise of the National Cyber Security Centre and the Centre for the Protection of National Infrastructure.

We will help the sector improve their operational resilience, including through exercises involving industry. We will also continue to improve our collective incident response capability and work closely with our international partners to develop our understanding of evolving threats to the global financial system.

Food Sector

Department for Environment, Food and Rural Affairs

The UK food sector has a highly effective and resilient food supply chain, owing to the size, geographic diversity and competitive nature of the industry. Although there is recognised dependency on other critical services, the resilience of the sector has been demonstrated by the response to potentially disruptive challenges in recent years.

Assessment of Existing Resilience

Like many industries, the food sector operates just-in-time supply chains which require sophisticated logistics operations and contingency plans to respond rapidly to potential disruption. The industry remains highly resilient owing to the capacity of food supply sectors and the high degree of substitutability of foodstuffs.

This resilience has been demonstrated in the response to events such as the 2015 flooding, and disruption to cross-channel transportation, the 2009 H1N1 Pandemic, the 2010 Icelandic volcanic ash clouds, the 2012 potential industrial action by fuel tanker drivers and severe winter weather experienced over the years 2010–2014.

Defra has well established mechanisms for engagement with industry. It has been working with the food industry sectors, across government and with the Devolved Administrations, to undertake contingency planning for a range of EU exit scenarios, including a no-deal scenario.

Building Resilience

Government and the sector will continue to work together to ensure the resilience of food supply. This will include:

- Building on recent research into the resilience of food supply with the Food Chain Emergency Liaison Group to respond to and recover from maritime transport disruption resulting from a major coastal flooding event;
- Building resilience in supply chains to extreme weather events; and
- Providing good practice guidance on cyber security. Last November, Defra published guidance on protecting food and drink from malicious attack, which includes specific advice on cyber security. The latest guidance can be found on the FSA's website at: https://www.food.gov.uk/news-updates/news/2017/16698/updated-advice-for-businesses-on-protecting-food-and-drink-supply

Defra has commenced a review of the UK Food Security Assessment (last published in 2010), to update and refresh the suite of indicators within it. The UKFSA is a comprehensive analysis of all aspects of food security.

Government Sector

Cabinet Office

Government provides a range of essential services through various infrastructure across the UK. Cabinet Office and the lead departments have developed a sound understanding of the risks the sector faces. A broad range of measures are in place which are kept under regular review to counter developing threats and ensure the sector and the electoral systems are as secure and resilient as possible. Cabinet Office will continue to fulfil a coordinating role to support departments to ensure central security and resilience efforts are appropriately directed and information is shared across the sector.

Assessment of Existing Resilience

- Major risks identified across the sector include malicious cyber activity, acts of terrorism, and other criminal activity, as well as technical failures. The breadth of these concerns requires a range of security and resilience measures to be adopted by the sector requiring education, training and exercising.

- Preventing and mitigating the impact of cyber incidents remains a significant challenge for the government sector, and substantial work has been carried out as part of the National Cyber Security Strategy. To ensure that the UK remains at the forefront of actively preventing and tackling malicious behaviour, the government has committed further investment in cyber security and is already benefited from the expertise in the National Cyber Security Centre.

- Government is transforming how security is delivered within departments to promote a robust security culture and are best able to respond to both current and future threats. Improvements have already been made through the introduction of clustered shared services which provide consistent and high standards of expertise and supported with a bespoke training programme.

Building Resilience

Security in government will continue to evolve and a rolling programme of assessment is in place to identify new vulnerabilities as well as measures to further strengthen mitigations against the risks and hazards this sector faces. The security and resilience of our electoral mechanisms will continue to be a priority focus. Departments will be accountable for ensuring they have effective personnel, physical and cyber security to defend against hostile foreign intelligence activity to agreed standards. Improvements in working with the commercial sector will help to deliver increased security assurance from suppliers.

Cabinet Office continues to engage as appropriate with Devolved Administrations to ensure joined up and mutually supportive programmes and, share expertise.

Health Sector

Department of Health and Social Care

The health and social care sector is diverse and needs to be resilient to a wide range of risks and disruptive challenges which may affect its ability to deliver services, whilst also ensuring it is able to deal with any resulting casualties. The sector has a wide scope including acute care, ambulance services, primary care, social care, and many arm's-length bodies including Public Health England, NHS Blood and Transplant and NHS Supply Chain.

Assessment of Existing Resilience

The **NHS** and **Public Health England (PHE)** have good levels of resilience and business continuity and an ability to divert resources from non-essential services in order for life-saving treatment to continue; similar principles apply to the resilience of the ambulance service. **NHS Blood & Transplant** routinely deals with surges in the demand for blood.

Although there is resilience within the system and local arrangements are effective in response, the **social care sector** is more challenging to understand. Continuous further work is being undertaken with local government, the providers and voluntary sector representatives to consider emerging issues regarding emergency planning, communication and information flows.

Over the last 12 months, DHSC and the health sector has responded to a number of significant incidents including the fire at Grenfell Tower, terrorist attacks and the WannaCry cyber-attack. Following these incidents, the sector has identified key lessons learnt and disseminated this knowledge.

Building Resilience

Throughout 2019/20, health organisations in England will continue to ensure that they have their own plans based on national and local risk assessments, and also joint plans and processes related to key dependencies, infrastructure, utilities, the workforce and the supply chain. Lessons identified from real incidents will be captured and shared.

The Department of Health and Social Care will be working with the sector to review and develop sector resilience to prolonged electricity supply disruption, cyber security and major adult social care provider failure amongst other risks. The department will also be strengthening its response capability to manage mass casualties.

Space Sector

Department for Business, Energy and Industrial Strategy

The space sector consists of Earth Observation, Satellite Communication, Global Navigation Satellite Systems and Space Situational Awareness services. All of these provide vital services for the day-to-day activity of the UK, such as landing aircraft safely at the airport, forecasting the weather and receiving live news reports from the other side of the world.

Assessment of Existing Resilience

The UK Space Agency is a currently building a picture of the risks to space services in the UK and how loss of these services could impact the space sector as well as other Critical National Infrastructure (CNI) sectors. The risks that the Agency will be assessing include cyber, physical & personnel, severe weather, power outages and loss of key staff.

The Agency will work with infrastructure owners and operators, as well as the end product users, to ensure that the critical infrastructure is resilient, and any issues are resolved in a manner proportionate with the risk. The anticipated future rapid expansion of the sector will bring additional challenges, and the Agency will work to embed resilience as a core consideration.

Building Resilience

Priorities include:

- Identifying the key dependencies on space services and assets within other Critical National Infrastructure sectors.
- Identification of the space sector critical assets and services.
- Identify and mitigate the risks posed to the critical assets and services to increase resilience in the sector.

The Outer Space Act 1986 created a licensing regime for the launching or operating of space systems, or any other activities in outer space. The Space Industry Bill is being developed to enable commercial spaceflight from UK spaceports. This regulates space, sub-orbital and associated activities and includes new powers and regulation to manage risk and ensure commercial spaceflight from the UK remains safe. This includes measures to regulate unauthorised access and interference with spacecraft, spaceports and associated infrastructure.

Transport Sector

Department for Transport

The transport sector comprises the road, aviation, rail and maritime sub-sectors. The majority of transport operates on a commercial basis, with responsibility for resilience devolved to owners and operators. The Department for Transport (DfT) works closely with stakeholders, including industry, to develop a common assessment of risks and ensures that proportionate and cost-effective mitigations are in place to reduce the likelihood. The department works closely with the British Transport Police and Maritime and the Coastguard Agency to deliver effective emergency response to, and mitigation against, security and resilience hazards.

Assessment of Existing Resilience

The scale and exposed nature of the transport network makes it vulnerable to some significant risks, such as severe weather. However, multi-agency emergency planning, investment in engineering and technological solutions, and the interconnected nature of transport networks all lend resilience to the sector.

Building Resilience

DfT's focus is on risks which have the highest impact or which have the biggest capability gaps. The Department's current priorities include:

- Security: The department engages with industry, cross-government colleagues and international partners to put in place effective and proportionate mitigation measures to protect the transport network.
- Incident response: The department works with the intelligence community, other departments, local responders and industry and has well-exercised internal response procedures.
- Cyber incident: The department has an active cyber security programme, working closely with industry as well as government and international partners to identify and mitigate cyber risks and vulnerabilities across all transport modes.
- Climate change and severe weather: As part of the 2016 National Flood Resilience Review, the department is working to identify local road networks in England that are at risk of flooding to provide an assessment of the impact of roads/bridges on communities if they are unavailable. Network Rail is developing route resilience plans to identify areas vulnerable to flooding.
- Industrial action: This can cause significant disruption to the travelling public across all the transport sub-sectors. We are working with industry and lead government departments to understanding the risk and mitigate the impact on the public and wider industry.
- Severe space weather: We are engaging with a number of government and industry stakeholders to build awareness and plan for the impacts of space weather on transport control, navigation and communication systems.

As part of the resilience work, DfT has a specific engagement programme with industry on winter weather resilience; delivers targeted research programmes to provide evidence to support policy development; and maintains collaborative relationships with industry.

Water Sector

Department for Environment, Food and Rural Affairs

An all-risks regulatory framework, effective mutual aid arrangements and high levels of investment continue to strengthen the resilience of the water industry to major disruptive events.

Assessment of Existing Resilience

- Irrespective of the risk, water companies are required by law to plan to provide water by alternative means in the event of a failure of the mains supply.

- The piped water supply system is generally resilient to the loss of individual facilities, and there is a widespread ability to reroute supplies from other parts of networks.

- However disruption to electricity supplies or widespread flooding could result in the loss of mains water and affect the movement and treatment of sewage. Water companies have contingency plans in place which include the use of back-up generators.

- Emergency response is bolstered by industry-wide and local mutual aid agreements to enable the sharing of resources between companies.

- All companies maintain statutory plans to minimise the impact of a drought.

- Defra has well established mechanisms for engagement with the water sector and we have been working with them, across government and with the Devolved Administrations, to undertake contingency planning for a range of EU exit scenarios, including a no-deal scenario.

Further Information

Links to some additional information relevant to the SSRPs are provided below:

- The National Security Strategy and Strategic Defence and Security Review (NSS & SDSR) describes the UK's national security objectives and interests, and how they will be delivered.

- The National Risks Register (NRR) describes significant risks, including malicious threats and natural hazards, that could affect the UK.

- The National Cyber Security Strategy 2016-2021 sets out HMG's strategy for tackling cyber security risks.

- Further information on cyber security is available on the National Cyber Security Centre's website.

- Further information on protective security is available on the Centre for the Protection of National Infrastructure's website.