Department
for Transport

Aviation Cyber Security Strategy

Moving Britain Ahead

The Department for Transport has actively considered the needs of blind and partially sighted people in accessing this document. The text will be made available in full on the Department's website. The text may be freely downloaded and translated by individuals or organisations for conversion into other accessible formats. If you have other needs in this regard please contact the Department.

Department for Transport
Great Minster House
33 Horseferry Road
London SW1P 4DR
Telephone 0300 330 3000
Website www.gov.uk/dft
General enquiries: https://forms.dft.gov.uk

Contents

Executive Summary 5
Introduction 6
- Why this strategy is needed 6
- What this strategy seeks to achieve 6
- Who is this strategy for 7

UK aims and priorities 8
- Alignment with the National Cyber Security Strategy 8
- Alignment with the Department for Transport's Aviation Strategy 9

Strategic Context 10
- The cyber threat to the UK 10
- The cyber threat to civil aviation 10
- International context 11
- Emerging Technologies 12

Roles and Responsibilities 13
- Government 14
- Regulators 15
- Industry 15

The way ahead 17
How we will achieve our aims 18
- a. Developing a comprehensive understanding of the cyber vulnerabilities across the aviation sector 19
- b. Continuously managing cyber risks 19
- c. Reporting and managing incidents, sharing information 23
- d. Working collaboratively at a global and European level 24
- e. Skills, training and resources 25
- Next steps 26

Annexes 27
- Annex A - Acronyms 27
- Annex B - Glossary 28

Annex C - International Organisations 30
Annex D - Incident reporting 31
Annex E - Index of Available Resources 32

Executive Summary

The aviation sector plays a critical role in allowing the people and businesses of the UK to travel and prosper, both domestically and around the world. Every day, millions of people rely on the safety, security and resilience of airlines, airports and the systems that support them, in order to be able to go about their business.

Feedback from the aviation industry, on the current cyber security advice and guidance for the sector, is that although useful clarity is needed from government to provide a path to becoming more secure. This Aviation Cyber Security Strategy aims to provide that clear path up to 2021/22 and aligns with HMG's National Cyber Security Strategy, and the Department for Transport's 2050 Aviation Strategy, to encompass advice and guidance already being used by the sector.

It is clear that there are dependencies between cyber, physical and personnel security, therefore this strategy champions a joined up approach between government, regulators and industry, to tackle current and future cyber-attacks or system compromises. The roles and responsibilities of each are clearly set out to ensure a robust approach to risk management.

As the aviation industry grows and new technology emerges, the cyber threat will adapt. This strategy, therefore, will be reviewed regularly to address changes to the cyber threat, technology and regulation. The strategy also aims to nurture new technology by encouraging a regulatory environment that does not stifle innovation, but works towards ensuring security by design and cyber resilience from the outset.

The approach to ensuring cyber security will continue to be collaborative and supportive and aim for the vision that **the UK's transport sector remains safe, secure and resilient in the face of cyber threats, and able to thrive in an increasingly interconnected, digital world**.

Introduction

Why this strategy is needed

1. Over decades a mature process of regulation and practice has been built up to safeguard civil aviation against the risks it faces, whether those be from mechanical or platform failure, collision, human error or terrorist attack. As the sector comes to rely more and more on complex and networked electronic information and communication systems, those systems must likewise be protected against the deliberate or accidental compromise of confidentiality, integrity or availability, that might put them, and the services they enable, at risk.

What this strategy seeks to achieve

2. This strategy sets out a path, up to 2021/22, to keep the UK civil aviation sector secure and resilient against malicious and unintended interference with information and communication systems. It complements the National Cyber Security Strategy[1] by setting out clear expectations, what roles the industry, Government (HMG), and regulators need to play, and what support HMG will offer. It has been produced in collaboration with the National Cyber Security Centre (NCSC), the Centre for the Protection of National Infrastructure (CPNI), and the Civil Aviation Authority (CAA), and in consultation with the UK aviation industry, to set stretching but achievable ambitions to address the risks to safe and secure operation of civil aviation.

3. Success at a strategic level will be the demonstrable transformation of the civil aviation industry's approach to cyber security (the ability to deter and protect against a cyber-attack or system compromise) and its cyber resilience (the ability to detect, contain, mitigate the effects of, defeat and recover from a cyber-attack or system compromise, including by switching to reversionary systems or means of operating if necessary) through the maintenance of robust risk management regimes. Operational success will be the continued safe and secure operation of civil aviation in the face of growing cyber threats and new and existing vulnerabilities. Tactical success will be an increasing capability, capacity and agility of stakeholders to deal with all aspects of the cyber security challenges faced by the UK civil aviation sector.

[1] https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

Who this strategy is for

4. This strategy sets out the Government's sector-level plan for aviation and outlines a framework within which the whole UK aviation industry can work with HMG and the regulators to manage the risk from malicious and unintended interference with information and communication systems. Its scope covers the whole of the UK aviation sector, including airports, operators of passenger and cargo services, air navigation service providers, manufacturers and other ancillary service providers. However this is a broad and diverse sector that incorporates a range of different entities, which cross international boundaries, and for which there is no single regulatory framework. Aspects of the strategy will be more relevant to some parts of the sector than others, but the core principles and guidance will be of interest to all.

5. The strategy is relevant not just to the owners and operators of critical national infrastructure (CNI) and the providers of essential services to the nation. Cyber security should be a priority for all parts of the sector, regardless of size or type of business. While some Government activity will necessarily be geared towards the most critical operators, particularly in respect of protecting resilience, the connectivity and interdependencies that exist within the sector mean that any weak link in the chain can potentially result in widespread disruption, economic impact and potential safety risk not just for that entity, but across the sector.

6. Cyber-attacks and compromise of systems can range in severity from website defacement to sophisticated attacks against, or catastrophic failure or compromise of, safety-critical systems. The Government's principal concern is in preventing any attack or compromise which poses a threat to the UK's national security, or affects the continued safe and secure operation of the UK's transport sector. All transport operators should have measures in place to mitigate against a range of attacks, including unsophisticated, low level attacks or compromises that do not have an operational or financial impact. The level of support provided by HMG in the event of a cyber-attack or system compromise will be dependent on the scale of its impact and sophistication.

UK aims and priorities

7. The overall vision of the DfT's cyber security programme is that **the UK's transport sector remains safe, secure and resilient in the face of cyber risks, and able to thrive in an increasingly interconnected, digital world.**

8. To realise this vision in the UK aviation sector, through this strategy we will work to achieve the following aims:

   Understand the risks posed by cyber threats to and vulnerabilities within the transport sector, and their potential consequences;
   Manage cyber risks and take appropriate and proportionate action to protect key assets;
   Respond to and recover from cyber events and incidents effectively and ensure that lessons are learnt;
   Promote cultural change, raise awareness and build cyber capability.

Alignment with the National Cyber Security Strategy

9. The UK's updated National Cyber Security Strategy is based on three broad objectives:

   DEFEND We have the means to defend the UK against evolving cyber threats, to respond effectively to incidents, to ensure UK networks, data and systems are protected and resilient. Citizens, businesses and the public sector have the knowledge and ability to defend themselves.

   DETER The UK will be a hard target for all forms of aggression in cyberspace. We detect, understand, investigate and disrupt hostile action taken against us, pursuing and prosecuting offenders. We have the means to take offensive action in cyberspace, should we choose to do so.

   DEVELOP We have an innovative, growing cyber security industry, underpinned by world-leading scientific research and development. We have a self-sustaining pipeline of talent providing the skills to meet our national needs across the public and private sectors. Our cutting-edge analysis and expertise will enable the UK to meet and overcome future threats and challenges.

10. For the most part, this strategy sits within the DEFEND objective, with a focus on supporting the aviation industry to manage their cyber risks, but in developing a UK aviation sector that is safe, secure and resilient to cyber risks, and has the requisite cyber skills to manage those risks, we are also addressing the DETER and DEVELOP objectives.

Alignment with the Department for Transport's Aviation Strategy

11. The DfT is creating a new Aviation Strategy to set out the long-term direction for aviation policy making for 2050 and beyond. In doing so, it will pursue the following aim:

To achieve a safe, secure and sustainable aviation sector that meets the needs of consumers and of a global, outward-looking Britain.

12. The strategy will have six objectives. These are to:

a) Help the aviation industry work for its customers;
b) Ensure a safe and secure way to travel;
c) Build a global and connected Britain;
d) Encourage competitive markets;
e) Support growth while tackling environmental impacts;
f) Develop innovation, technology and skills.

13. This Aviation Cyber Security Strategy will directly contribute to DfT achieving objective b) of ensuring a safe and secure way to travel. It will also facilitate objectives c) and f) by helping to ensure that we build a technological and regulatory environment which helps foster the development of emerging technologies in the UK and does not stifle innovation.

Strategic Context

The cyber threat to the UK

14. The Government is clear that the cyber threat to the UK is increasing and becoming more dynamic and unpredictable. A number of threat actors including criminals, state actors, terrorists and hacktivists can use cyberspace to exploit vulnerabilities and cause damage.

15. Malicious insiders, who are trusted employees of an organisation and have access to critical systems and data, can also constitute a significant vulnerability if they use their privileged knowledge or access to facilitate or perpetrate a criminal act or attack. The Centre for the Protection of National Infrastructure (CPNI) provides specific advice on reducing the insider risk through personnel and people security, and advice on the mitigation of physical security vulnerabilities.[2]

16. There is scope for considerable economic and social disruption from malicious attacks, from denial of service and data breaches to the compromise of safety critical systems which in extreme cases could cause risk to life. Technological advancements are liable to increase opportunities for hostile actors who will become more innovative in developing malware and delivery methods.

The cyber threat to civil aviation

17. Like all of the UK's National Infrastructure, the UK aviation sector has been and will continue to be a potential target for cyber-attacks. These may occur across the multitude of different systems, platforms and technologies that facilitate safe and efficient travel.

18. Aviation is already a known target for international terrorist groups, as repeated attempts to destroy aircraft using explosive devices have shown. No examples have been found of specific terrorist cyber threats against the aviation sector, and risk assessment work carried out by the International Civil Aviation Organisation (ICAO) and in the UK has concluded that the risk of a successful terrorist cyber-attack causing loss of life is low compared to other possible types of terrorist threat.

19. There is a higher and ongoing risk of cyber-attacks or compromises that could cause disruption to aviation services. While the human and long-

[2] https://www.cpni.gov.uk/personnel-and-people-security

term economic impact of such incidences would not be as severe, the commercial, operational and reputational impacts could still be highly damaging.

20. Finally, the risk of espionage must not be underestimated. This may be conducted by a variety of actors in order to disrupt service, obtain commercial advantage, customer data for criminal activity or to release data (such as emails) which may cause reputational damage. Information gathering on infrastructure and employees may also contribute towards planning physical attacks or further cyber-attacks on the aviation sector.

What is cyber security?

"'Cyber security' refers to the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures."
Source: National Cyber Security Strategy

International context

21. While the DfT's aviation policy responsibility is focused on the UK aviation sector, aviation is a truly global business. This means we have a significant interest in shaping international approaches, standards and practice by establishing and maintaining strong, active relationships with partners; using our influence with multilateral organisations and developing a coherent international aviation cyber security threat and vulnerability picture, including improving understanding of the global reach of aviation interconnections, and how they interface with national systems.

22. There are a large number of organisations at European and international levels who each have a role to play in shaping the global approach to cyber security. **Annex C** provides a list of organisations that covers the major players responsible for devising regulation and guidance at an international level.

The UK's exit from the European Union (EU)

23. Aviation security is an area where the UK has historically had a significant influence on European policy, having been in the forefront of the development and use of many anti-terrorist strategies. We have used our membership of the EU to advocate, with considerable success, tighter and

more responsive security rules across Europe. Upon exiting the EU the UK will retain the EU Regulations which help to keep us safe from cyber-attacks; one such example is keeping in place the Network and Information Systems (NIS) Directive (see page 21) which ensures operators of essential services have in place a robust set of minimum cyber security measures.

24. Given that 75% of international passengers arrive from Europe, those highly effective standards will continue to provide protection for a large number of UK citizens. The UK will continue to positively influence European standard-setting organisations such as the European Civil Aviation Conference (ECAC) and the European Organisation for Civil Aviation Equipment (EUROCAE) (see **Annex C**) to ensure that cyber security remains a priority and, where possible, to exchange information. On an international level, the UK will remain represented at ICAO (see **Annex C**) and push for strong cyber security standards at a global level. Parallel to working with and within these organisations, the UK will pursue its current bilateral relations as well as forge new ones.

25. Keeping British nationals safe is our top priority and we will continue to work collaboratively at an international level to make sure we do just that.

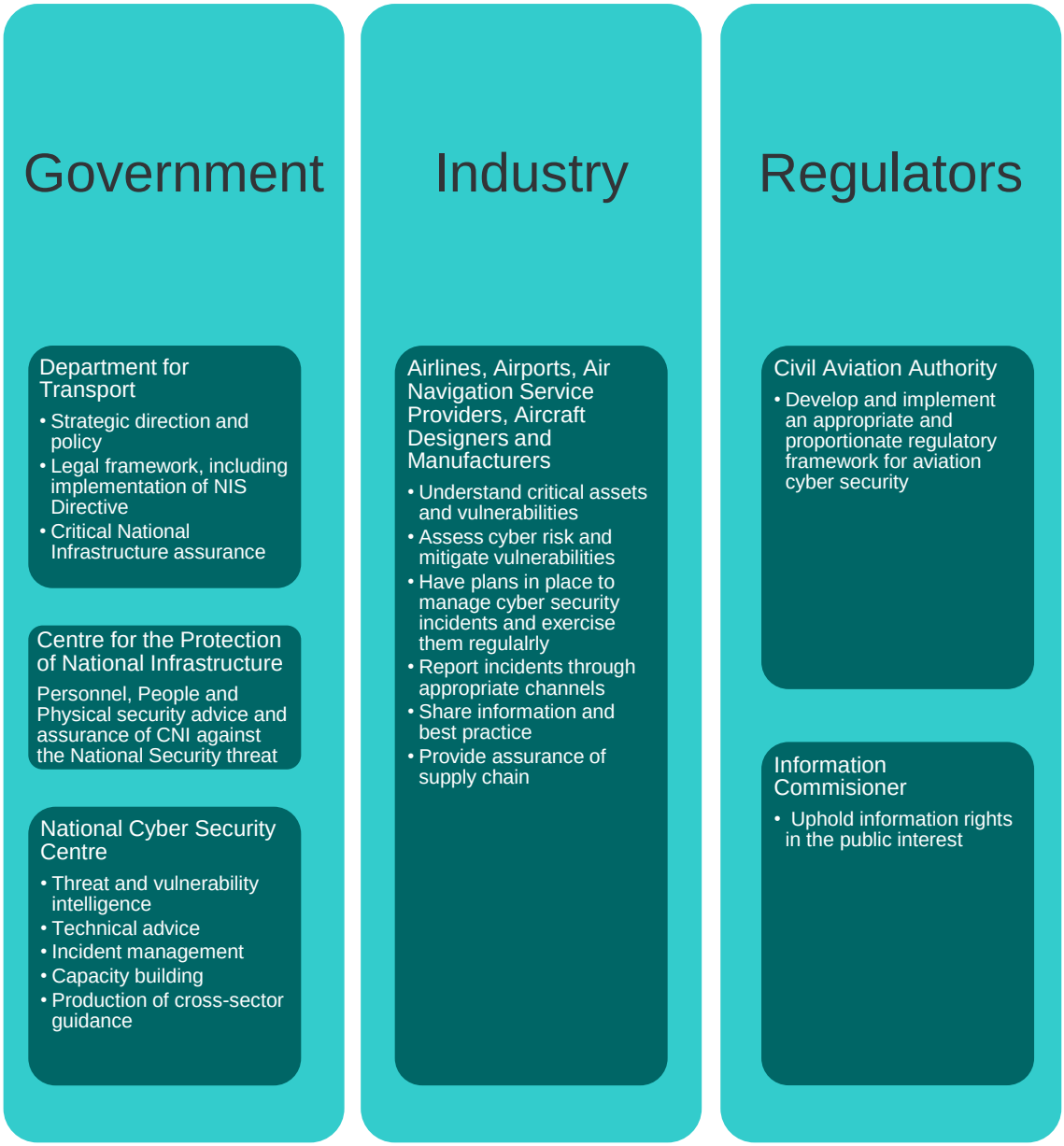
Emerging Technologies

26. Once considered to be the stuff of science fiction, Unmanned Aerial Systems (UAS) are already being used to improve and deliver services in our everyday life. They offer exciting opportunities for organisations to improve services, create high tech jobs and have significant potential to boost the economy across the UK. We want to build a technological and regulatory environment which helps foster the development of the UAS market in the UK and does not stifle innovation.

27. However, like many other technologies, UAS can be misused and present challenges to safety, security and privacy. If cyber security is not considered from the start of the design process, the attractiveness and potential for malicious actors to hack into larger and more capable UAS systems to use them for unlawful or destructive means will increase. This will also apply to the next emergent technologies within aviation, be that spaceplanes, hypersonic aircraft, future air traffic management systems or future fuel technologies; cyber resilience needs to be built into the future innovations from their conception.

Roles and Responsibilities

26. Efficiently and effectively mitigating the current and future risks of a cyber-attack or systems compromise in the UK's aviation sector requires a joined up approach between the Government, regulators and the aviation industry. It is a balance of the right legislative framework, timely and accurate intelligence, robust risk management and the capability to respond to and recover from incidents when they occur. There are also considerable dependencies between cyber security, physical security and personnel security, so a holistic approach is necessary to ensure that each risk is managed appropriately. The key roles of each of the partners in delivering this can be illustrated in the following diagram:



Government

The Department for Transport

27. DfT is responsible for setting the strategic direction of aviation cyber security policy and regulation across government and industry, tailoring our response and resources to the likelihood of an incident or event occurring and its potential impact. This will be based on a robust assessment of the cyber security risks to the transport sector, grounded in DfT's 'all-risks' approach to transport security – considering the risks of terrorism and natural/civil hazards in addition to cyber.

28. While the cyber risk to civil aviation is to assets, facilities, systems, platforms, networks, processes and people largely owned and managed by the private sector, as well as the general public, DfT's role is to provide advice, guidance and regulation (mainly through the CAA) to help operators and owners to mitigate the risk. DfT is also responsible for taking steps to ensure that Critical National Infrastructure in the transport sector is appropriately and proportionately protected from cyber-attack.

The National Cyber Security Centre (NCSC)

29. The Government set up the NCSC to be a single, central body for cyber security at a national level. The NCSC is responsible for:

    - providing an authoritative voice and centre of expertise on cyber security;
    - working hand in hand with the aviation industry, academic and international partners to keep the UK secure in cyberspace;
    - analysing, detecting and understanding cyber threats;
    - managing national cyber incidents;
    - delivering tailored support and advice to Lead Government Departments, the Devolved Administrations, regulators and businesses, including through the production of guidance; and
    - providing its cyber security expertise to support the Government's efforts to foster innovation, support a thriving cyber security industry, and stimulate the development of cyber security skills.

Centre for the Protection of National Infrastructure (CPNI)

30. CPNI is the government authority for protective security advice relating to national security threats in the physical and personnel / people security areas. Its role is to protect national security by reducing the vulnerability of the Critical National Infrastructure and other assets subject to national security threats. CPNI provides advice on physical security and personnel

and people security, which should form part of a multi-layered approach to managing cyber risks.

Regulators

The Civil Aviation Authority (CAA)

31. The CAA is responsible for the regulation of aviation safety in the UK, monitoring compliance by the industry with aviation security requirements, determining policy for the use of airspace, the economic regulation of Heathrow, Gatwick and Stansted airports, the licensing and financial fitness of airlines, regulation of UK initial airworthiness activities that fall outside the remit of Europe, oversight of continued and continuing airworthiness activities in the UK, and the management of the ATOL financial protection scheme for holidaymakers. Considering the security responsibilities of the CAA, they have been tasked by DfT to develop and implement a regulatory framework for cyber security, also, to facilitate oversight of industry's activities related to mitigating potential cyber risks to civil aviation in the UK.

Information Commissioner's Office (ICO)

32. The role of the ICO is to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. In the context of cyber security in aviation, the ICO is responsible for enforcing the Data Protection Act 2018 and the General Data Protection Regulation (including within the aviation industry), and the protection of its data.

Industry

The UK Aviation Industry

33. The UK aviation industry is responsible for the ownership and management of the cyber risks to their organisations at board level, as they are with any other security risk. This includes responsibility for meeting the required regulatory standards set by HMG and the CAA. Each organisation must ensure that they know what their critical assets are, that their vulnerabilities are understood and mitigated, that cyber security risks are assessed and managed appropriately and proportionately, and that incidents and events are reported through the appropriate channels (see **Annex D**).

34. Organisations must have robust cyber incident response plans in place, these plans should be tested and updated on a regular basis, with

mechanisms put in place to implement lessons learned from exercises and real life incidents.

35. These activities must be extended to include the organisation's supply chain and partners. All organisations, including system, equipment and aircraft designers, manufacturers, sub-contractors, suppliers and potential 3rd parties, should work together to enhance the cyber security of the whole aviation system. Finally, the aviation industry should promote a cyber security culture, and ensure that all staff, from the operational to the board level, have an appropriate level of understanding of the cyber security risks that their organisation manages.

The way ahead

What we aim to deliver and when

Year 1

2017 - 18

Government

- Programme of targeted technical assessments of Critical National Infrastructure sites and other critical assets.
- Internal crisis response plans and advice for industry on reporting incidents.
- Building of threat and risk picture with industry input.
- Development of a network of cyber contacts in HMG, the regulator and the aviation industry.

Regulator

- Development of regulatory framework and consultation with industry on proposed phased approach and incorporation into charging regime.

Industry

- Increasing senior executive understanding and ownership of cyber security risk.
- Development of appropriate and proportionate risk management processes and procedures.
- Increase in levels of incident monitoring and reporting.

Year 2-4

2018 – 2020/21

Government

- Established incident response mechanism including clear lines of reporting and implementation of lessons learned.
- Implemented the NIS Directive and published accompanying Guidance.
- Comprehensive programme for industry, HMG and the regulator to test and exercise response and resilience plans.
- An established cyber risk assessment process.
- Emerging findings report for the wider aviation industry on cyber vulnerabilities and advice on how to mitigate them, based on the technical assessments from Year 1.

Regulator

- Implementation and embedding of regulatory framework across aviation, including delegated aspects of the NIS Directive.

Industry

- A developed, outcome focused approach to managing cyber risks, using government or private sector support if required, as part of a holistic cyber (and overall) security stance.

Year 5

2021 - 22

A set of durable arrangements between industry, HMG, the regulator and other authorities that allows for genuine collaboration and an effective evolution of response to cyber risks.

Government

- The mainstreaming of cyber security alongside other security risks.

Regulator

- A robust and flexible regulatory regime for aviation cyber security.

Industry

- A mature approach to understanding cyber risks and delivering outcome focussed solutions which are approved by the regulator.

How we will achieve our aims

37. Each element of our approach below contributes to achieving one of our four aims:

AIM:	APPROACH:
Understand the risks posed by cyber threats to and vulnerabilities within the transport sector, and their potential consequences.	a. Developing a comprehensive understanding of the cyber vulnerabilities across the aviation sector. It is impossible to mitigate against vulnerabilities without knowing what they are. HMG will remain engaged with the aviation industry to understand these vulnerabilities usually through Cyber Risk Reviews.
Manage cyber risks and take appropriate and proportionate action to protect key assets.	b. Continuously managing cyber risks. As HMG gains a better understanding of the cyber vulnerabilities and technology advances, the approach to managing the cyber risks must remain flexible and the approach regularly refreshed.
Respond to and recover from cyber events and incidents effectively and ensure that lessons are learnt.	c. Reporting and managing incidents, sharing of information.
Promote cultural change, raise awareness and build cyber capability.	d. Working collaboratively at a global and European level. The UK has a significant interest in shaping international aviation standards and practices. Therefore HMG will continue to represent the UK's ambitions at an international level. e. Skills, training and resources. HMG has committed to tackle the systemic issue of a shortage of cyber skills. A number of initiatives have been implemented (see **Annex E**) to encourage more people into the profession.

a. Developing a comprehensive understanding of the cyber vulnerabilities across the aviation sector

38. For a cyber risk to materialise, not only must there be an extant threat, but also a vulnerability to exploit. It is impossible to mitigate those vulnerabilities without first understanding what they are, thus much of HMG's work with infrastructure operators to date has been in seeking to understand these vulnerabilities, what kinds of systems and platforms are critical to different types of organisation and what the impact of the loss of confidentiality, integrity or availability of them would be, often in the form of direct engagement and formal Cyber Risk Reviews.

HMG will deliver:

- An ongoing, targeted series of technical assessments of Critical National Infrastructure sites and other critical assets, including data and information systems;
- An emerging findings report for the wider aviation industry outlining common vulnerabilities and how they can be mitigated, based on the targeted technical assessments.

The UK Aviation Industry will:

- Identify and maintain a list of all their critical digital, IT and OT systems, platforms and technologies across their organisation and their supply chain;
- Have a clear understanding of why those assets are critical to their organisation, and where their potential vulnerabilities lie.

Outcome:

Mature understanding between and within HMG, the regulators and the industry of both specific vulnerabilities in Critical National Infrastructure sites and other critical assets, and common vulnerabilities across the sector.

b. Continuously managing cyber risks

i. Risk management

39. As we develop a better understanding of the cyber vulnerabilities, systems, platforms and the potential consequences of a loss of confidentiality, integrity or availability of them on the aviation sector, we must seek to manage those cyber risks. Technological advancements are continuing to change the environment within which the UK aviation sector operates, so

we must be flexible and adapt and refresh our approach regularly, while seeking to mainstream cyber security with other security and safety risks.

HMG will deliver:

- Targeted support and advice to industry partners on their mitigation plans;
- National level cyber risk assessment, and promulgation of the results through high-level briefings to Boards and industry groups to raise awareness about the issues and steps industry can take to protect itself against specific threats, and understand the potential cost to business of a cyber-attack or system compromise;
- Guidance for manufacturers of airport screening equipment on how to build equipment that is more resilient and secure from cyber-attack and system compromise;
- Guidance for operators of airport security screening equipment on how to maintain the security of networked systems throughout their service and advice to the security staff operating the equipment;
- Comprehensive guidance on the NIS Directive for aviation operators within the scope of the Directive.

The UK Aviation Industry will:

- Implement a cyber security risk management regime that includes continuous identification and assessment of cyber risks, mitigation of vulnerabilities, robust governance structures and risk ownership.
- Ensure that cyber risks are managed throughout the lifespan of any new and developing systems, platforms and technologies.

The Directive on the Security of Network and Information Systems (NIS Directive)

The NIS Directive was adopted by the European Parliament on 6 July 2016 and the UK NIS Regulations came into force on 10th May 2018.

The Directive is designed to boost the overall level of security for network and information systems that support the delivery of essential services within the EU. It applies to those sectors which are vital for our economy and society, providing services such as the supply of electricity and water and the provision of healthcare and transport.

The NIS Regulations place mandatory requirements on "Operators of Essential Services" (OES) to have measures in place to manage security risks, including incident notification, relating to the security of their network and information systems.

Competent Authorities are required to monitor the application of the NIS Regulations, which includes monitoring whether OES are meeting their security duties. This will be done through assessing the level of compliance of OES against security requirements.

DfT and the CAA are both acting as Competent Authority for the aviation sector and there is a clear division of roles and responsibilities between the two organisations. In summary, the CAA is the primary organisation with which the OES in the aviation sector will engage on a regular basis and it is intended that the Secretary of State for Transport will only be formally involved when enforcement action is required. Incident notifications will also be submitted to the DfT.

Outcome:

The UK aviation industry is provided with guidance and advice on how it can manage its cyber security risks and protect itself from cyber-attack or system compromise.

ii. Achieving the right balance of regulation, standards and guidance

40. There are areas where we believe regulation is required to protect the public from the risk of a destructive or disruptive cyber-attack or system compromise. In what is a complex regulatory landscape, it will also help give clarity around the measures we expect industry to have in place. Our focus remains on an appropriate and proportionate response to cyber risks, so we are not aiming to regulate in an overly prescriptive way, but to provide a balance between regulation, standards and guidance. This will be an ongoing and consultative process led by the CAA's Cyber Oversight Project.

The CAA Cyber Oversight Project

The vision of the CAA Cyber Oversight Project is for industry to have in place robust, flexible and dynamic mitigations to reduce potential cyber risks, supported by a proportionate regulatory oversight scheme. This will enable all aviation industry stakeholders to exploit the benefits of cyberspace without compromising aviation safety and continuation of service both now and in the future.

The Cyber Oversight Project will aim to:

- Develop an appropriate and proportionate regulatory framework, in consultation with the aviation industry and in doing so;
    - Oversee industry's efforts to mitigate the cyber risks to the UK aviation sector
    - Build and share aviation cyber security knowledge, skills and capability;
    - Foster international best practice in aviation cyber security;
    - Provide the travelling public with appropriate reassurance that the aviation industry is managing its cyber risks in a transparent way.

The Cyber Oversight Project will deliver:

- A proportionate aviation cyber regulatory framework that establishes clear roles and responsibilities across aviation stakeholders and manages security risks in an appropriate and proportionate manner;
- Clearly defined legal requirements that add clarity to aviation industry responsibilities and add, where necessary, the appropriate triggers to drive proper stakeholder behaviours;
- Standards, advice and guidance that is relevant to operators of all sizes to help aviation address the evolving cyber risk picture;
- Implementation of the NIS Directive for aviation, with the CAA and DfT acting as the Competent Authority, and the CAA assessing compliance.

The UK Aviation Industry will:

- Work in partnership with the CAA to support the development of an appropriate and proportionate cyber regulatory framework.

Outcome:

A mature and proportionate regulatory regime that supports the robust, flexible and dynamic mitigations adopted by industry to ensure the UK aviation industry manages potential cyber risks on an ongoing basis.

c. Reporting and managing incidents, sharing of information

41. It is not a matter of *if* but *when* cyber-attacks or system compromises are perpetrated against or impact upon the aviation sector. We must seek to ensure that the aviation industry is sufficiently prepared to deal with such incidences when they do occur, that there are clear lines of reporting and that lessons learnt are proactively shared across industry – all part of a robust risk management regime.

HMG will deliver:

- A report on industry's current and planned future capability to respond to a cyber-attack (undertaken recently by Helios Consulting), with future repeat assessments to be carried out periodically to monitor progress;
- Development of a comprehensive exercise programme for HMG, the regulator and industry;
- Clear reporting lines for incidents and advice on what to report and when (see **Annex D** - Incident Reporting);
- Threat information and intelligence via the Cybersecurity Information Sharing Partnership (CiSP);
- Support to industry in setting up aviation cyber security-specific networks and meetings for the purpose of information exchange and sharing of best practice.

The UK Aviation Industry will:

- Develop and implement robust cyber incident response plans and procedures that enable organisations to identify, manage, defeat and recover from a cyber-attack or system failure;
- Report incidents to HMG and the regulator through the appropriate channels as outlined in Annex D.

Outcome:

An established incident response mechanism including clear lines of reporting and processes for implementing lessons learned that enables Government and industry to respond quickly and effectively to cyber security incidents.

What is CiSP?

The Cybersecurity Information Sharing Partnership (CiSP) is a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business. Benefits include:

- engagement with industry and government counterparts in a secure environment
- early warning of cyber threats
- ability to learn from experiences, mistakes, successes of other users and seek advice
- an improved ability to protect company networks
- access to free network monitoring reports tailored to organisations' requirements

d. Working collaboratively at a global and European level

42. The UK has a significant interest in shaping international aviation standards and practice, and the steps below describe our specific aims for international engagement (see **Annex C** for further information about individual organisations). By and large, HMG will represent the UK's interests at an international level, but where appropriate, the CAA will also play a role in delivering our objectives in this area.

HMG will deliver:

- The UK will support the development of a coherent international risk picture for the aviation cyber security threat through ICAO's Working Group on Threat and Risk;
- The UK will work alongside other partners to help develop global approaches to tackling cyber vulnerabilities, and will continue to press for ICAO leadership in this area;
- The UK will seek to support and input to an appropriate pan-European forum for exchanging information and incident response;
- The UK will continue to support the work of the ECAC Study Group on the Cyber Threat to Aviation, and help to update and maintain ECAC guidance to states on cyber security;
- The UK will continue to support and input to the development of appropriate and proportionate aviation cyber security standards for industry through EUROCAE.

Outcome:

The UK is able to shape the global evolution of cyberspace in the context of civil aviation in a manner that advances our wider economic and security interests.

e. Skills, training and resources

43. In order for the UK aviation industry to have the capability to manage its cyber risks, we must tackle the systemic issues at the heart of the cyber skills shortage, which we know is negatively impacting aviation sector organisations' ability to act in some cases. Common challenges include the lack of young people entering the profession, the shortage of current cyber security specialists and the absence of established career and training pathways into the profession. An index of current initiatives, campaigns and resources is at **Annex E**.

HMG will deliver:

- The NCSC Industry 100 secondments initiative which invites organisations of all sizes to work with the NCSC by embedding staff into the organisation to provide industry with a greater understanding of the cyber security environment, and the NCSC with new perspectives and knowledge of different sectors;
- Access to certified training and professional schemes through the GCHQ Certified Training (GCT) scheme[3] and the NCSC Certified Professional (CCP) scheme[4].

The UK Aviation Industry will:

- Develop clearly defined career development paths and further development opportunities for cyber security professionals in the civil aviation sector. This will grow both the pool of suitably qualified and experienced cyber security personnel in the sector, as well as raising existing personnel's cyber security capability.

Outcome:

A self-sustaining pipeline of talent providing the skills to meet our national needs across the UK aviation sector. Our cutting-edge analysis and expertise will enable the UK aviation sector to meet and overcome future threats and challenges.

---

[3] https://www.ncsc.gov.uk/scheme/gchq-certified-training
[4] https://www.ncsc.gov.uk/scheme/certified-professional

Next Steps

44. It is intended that the deliverables outlined above will be revisited annually. This is both to assess the performance of all stakeholders, but also the relevance and effectiveness of the measures proposed as part of a flexible framework to manage cyber risks and the delivery of this strategy.

45. Some of the activities and deliverables outlined in the section above are already underway, while some will commence over the next couple of years. This strategy covers an initial 5 year period of activity, however cyber risks to the aviation sector will only continue to grow and diversify, so it is vital that we manage those risks appropriately and on an ongoing basis. Ultimately cyber risks are one category of a wide range of risks that the aviation sector faces – in order to protect the sector, we must take a holistic view of them all.

46. No organisation can tackle cyber risks in isolation; it is only by encouraging collaboration between and within HMG, the regulator and industry, on a domestic and international basis that we can successfully secure the UK's aviation sector.

Annex A – Acronyms

ANSP	Air Navigation Service Provider
ATM/ANS	Air Traffic Management/Air Navigation Service
CAA	Civil Aviation Authority
CiSP	Cybersecurity Information Sharing Partnership
CNI	Critical National Infrastructure.
CPNI	Centre for the Protection of National Infrastructure.
DfT	Department for Transport
EASA	European Aviation Safety Agency
ECAC	European Civil Aviation Conference
EU	European Union
EUROCAE	European Organisation for Civil Aviation Equipment
HMG	Her Majesty's Government
ICAO	International Civil Aviation Organisation
ICO	Information Commissioner's Office
IT	Information Technology
NCA	National Crime Agency
NCSC	The National Cyber Security Centre.
OT	Operational Technology
UAV	Unmanned Aerial Vehicle
UTM	Unmanned Traffic Management

Annex B – Glossary

Asset	The logical and physical resources of the civil aviation entity concerned, for example, for aircraft those which contribute to the airworthiness of the aircraft, including functions, systems, items, data, interfaces, processes and information.
CIA	**Confidentiality:** that data or information is not made available to unauthorized individuals, entities or processes. **Integrity:** the accuracy and completeness of data and information assets. **Availability:** the property of being accessible and usable upon demand by an authorised entity.
CNI	Critical National Infrastructure. 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.
Incident	The NCSC defines a cyber security incident as: • A breach of a system's security policy in order to affect its confidentiality, integrity or availability • The unauthorised access of attempted access to a system The NCSC defines a **significant** cyber security incident as one which may have: • Impact on the UK's national security or economic wellbeing • The potential to cause major impact to the continued operation of an organisation
Threat	The assessed likelihood or probability of an act of deliberate interference be, it a terrorist attack or other crime being attempted (target, type of attack, perpetrator) within certain time frame; A result of motivation, intent and means/capabilities.

Vulnerability	The features of something potentially under threat which can be exploited by an attacker e.g. at an airport or on an aircraft, or which mean the asset may be inadvertently effected by an deliberate act of interference against a non-aviation target, combined with any weakness in current security measures.

Annex C – International Organisations

The European Aviation Safety Agency (EASA) - an agency of the European Union whose principal objective is to establish and maintain a high, uniform level of civil aviation safety in Europe through its Basic Regulation.

The European Civil Aviation Conference (ECAC) - functions as the European branch of ICAO, and seeks to harmonise civil aviation policies and practices amongst its Member States and, at the same time, promote understanding on policy matters between its Member States and other parts of the world.

The European Organisation for Civil Aviation Equipment (EUROCAE) – EUROCAE works with its members and the aviation industry to develop industry standards for civil aviation that are recognised worldwide, and:

- Build upon the expertise of its members and address the global aviation challenges;
- Are fit for purpose to be adopted internationally
- Support existing operational, development and regulatory processes.

The International Civil Aviation Organisation (ICAO) - sets international civil aviation safety requirements in the form of Standards and Recommended Practices (SARPs), and provides an international framework for addressing “acts of unlawful interference”, which include disruptive as well as safety effects.

Annex D – Incident reporting

CYBER INCIDENT REPORTING GUIDANCE: AVIATION

THIS GUIDANCE DOES NOT REPLACE MANDATORY OCCURANCE REPORTING REQUIRED BY THE CAA.

	• SERVICES SERIOUSLY AFFECTED • ACTION NEEDED INTERNALLY TO CONTAIN AN INCIDENT	• SUSPICIOUS ACTIVITY DETECTED • SUCCESSFUL CYBER ATTACK ON NON OPERATIONAL SYSTEMS
Type of incident	There is a **significant impact on services** or a **risk to safety.** Potential or actual significant **impacts beyond your operations.** **Action** is required **to maintain or protect services.** Intrusions that appears to have **capability or intent to cause a failure of a service.**	**Any suspicious cyber activity that does not have actual or potential impact on service provision or safety.** *Examples could include: unauthorised attempts to gain access to systems, unauthorised use of systems and/or data, denial of service, etc.*
What you should do	**Always report these incidents to NCSC and DfT.** Report by email or telephone **as soon as possible** after detecting and in any case **within 72 hours**. **1. Contact NCSC first** 0300 020 0973 (24/7 contact number), incidents@ncsc.gov.uk **2. Contact DfT next – 24/7 Inc bank holidays** In office hours (09:00 – 17:30pm): 020 7944 6322, TSOC@dft.gsi.gov.uk Out of hours (17:30pm – 09:00am): 020 7944 6322, TSOC@dft.gsi.gov.uk **Report fraud, scams or extortion** through the Action Fraud Website: http://www.actionfraud.police.uk/ or **+44(0)300 123 2040** if you are **suffering a live cyber-attack** (24/7)	If possible **report within 72 hours** of detecting the event. The incident **could escalate!** **Report via CiSP**: https://www.ncsc.gov.uk/cisp Contacting NCSC and DfT is recommended. **Report fraud, scams or extortion** through the Action Fraud Website: http://www.actionfraud.police.uk/

- Organisations should check their reporting obligations under data protection legislation and related guidance. Under certain circumstances it will be necessary to notify the Information Commissioner's Office https://ico.org.uk/for-organisations/report-a-breach/
- If there is an impact on safety, organisations should also report the incident to the relevant safety regulator as per normal procedures
- Organisations that are in scope of the NIS Directive will have to follow additional mandatory requirements to notify the Competent Authority of incidents from May 2018.

Annex E – Index of Available Resources

Cybersecurity Information Sharing Partnership (CiSP)[5]

CiSP is a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business.

10 Steps to Cyber Security[6]

The 10 Steps to Cyber Security guidance is designed for organisations looking to protect themselves in cyberspace. Understanding the cyber environment and adopting an approach aligned with the 10 Steps is an effective means to help protect your organisation from attacks.

Cyber Essentials[7]

Under this scheme, which is backed by Government and supported by industry, organisations can apply for a badge which recognises the achievement of government-endorsed standards of cyber hygiene.

Cyber First[8]

CyberFirst is a Student Bursary scheme inspired and led by GCHQ which aims to help support and prepare students for a career in cyber security. GCHQ will partner with other government departments and selected industry to offer students a comprehensive package of financial assistance and cyber skills to help kick start a career in cyber.

Industry 100[9]

One of the key objectives of the National Cyber Security Centre (NCSC) is to reduce risks to the UK by working with public and private sector organisations to improve their cyber security. As part of Industry 100, we are inviting organisations of all sizes to work with us by embedding staff into the NCSC so we can achieve a greater understanding of the cyber security environment using wide and diverse thinking.

---

[5] https://www.ncsc.gov.uk/cisp

[6] https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

[7] https://www.cyberaware.gov.uk/cyberessentials/

[8] https://www.ncsc.gov.uk/articles/cyber-first-bursary-scheme

[9] https://www.ncsc.gov.uk/information/industry-100