UK Civil Aviation Authority

Cyber Security Enforcement Policy

CAP 3120

Published by the Civil Aviation Authority, 2025

Civil Aviation Authority
Aviation House
Beehive Ring Road
Crawley
West Sussex
RH6 0YR

First published February 2025
Issue 1 – June 2025

Enquiries regarding the content of this publication should be addressed to: cyber@caa.co.uk

The latest version of this document is available in electronic format at: www.caa.co.uk/CAP3120

Contents

1. Purpose

The Aerospace industry is a critical component of global infrastructure, necessitating stringent measures to ensure standards are maintained to protect against the growing threat from cyber-attacks to the safe, secure and resilient operation of the industry. This policy sets out the enforcement approaches used across the CAA to enforce safety, security, resilience and space regulations of which the Cyber Team has responsibility for the oversight of cyber security provisions. In addition, the policy highlights the importance that collaboration plays in ensuring continued compliance, essential to enhancing the cyber security posture of the UK aerospace industry.

The main objective of this policy is to provide a clear and transparent approach to how the Cyber Team responds to identified and suspected non-compliance for each of the regulations it has a shared oversight or Licensing and Monitoring responsibility for.

By adhering to this policy, the Cyber Team commit to ensuring that relevant stakeholders/teams who are accountable for the ongoing compliance of regulations are made aware and consulted on any non-compliance or suspected non-compliance with cyber security provisions at the earliest opportunity so that appropriate enforcement actions can begin by the responsible teams.

2. Introduction

The CAA Cyber Team works across capability areas including airworthiness, flight operations, aerodromes, air traffic management, aviation security and space to ensure cyber resilience, safety, and security of the aerospace sector. This includes supporting oversight, licensing and monitoring and enforcement of new and existing safety, security and resilience and space regulations designed to protect critical aerospace systems and data from cyber threats.

The enforcement approaches of the Department for Transport (DfT), the Safety and Airspace Regulation Group (SARG), Aviation Security (AvSec), and Space share several commonalities:

- **Engagement and Guidance**: Prioritise engaging with regulated entities to offer guidance, support, and resources that promote understanding and compliance with regulations.
- **Corrective Actions**: Address identified deficiencies by requiring the development and implementation of corrective action plans to resolve non-compliance issues.
- **Monitoring and Auditing**: Conduct regular monitoring and auditing to oversee deficiencies and corrective actions, ensuring continued adherence to regulations.
- **Enforcement Actions**: Implement enforcement measures, such as notices, restrictions, licence revocations, fines, or prosecution, to address non-compliance and deter future violations.

To address non-compliance, the Cyber Team will work collaboratively with the relevant SARG, AvSec, DfT and Space teams to encourage appropriate self-initiated remedial action by industry using the Cyber enforcement approach and where required, leverage existing CAA enforcement approaches to escalate enforcement.

3. Scope

This guidance applies to organisations who have regulatory obligations to comply with existing safety, security, resilience and space regulation.

Applicable regulations include, but not limited to:

Aviation Security

- National Aviation Security Programme (NASP) – Single Consolidated Direction 2/2024 - Chapter 13

Aviation Safety

- UK Reg (EU) No 139/2014 (the UK Aerodromes Regulation)
- UK Reg (EU) No 965/2012 (the UK Air Operations Regulation)
- UK Reg (EU) No 1321/2014 (the UK Continuing Airworthiness Regulation)
- UK Reg (EU) No 2017/373 (the UK ATM Provision of Services Regulation)

Operational Resilience

- Network and Information Systems (NIS) Regulation 2018

Space

- Space Industry Regulations 2021 (Regulations)

4. Cyber Enforcement Approach

Section 5 applies only to those organisations in scope of the following regulations:

- National Aviation Security Programme (NASP) – Single Consolidated Direction 2/2024 - Chapter 13
- Network and Information Systems (NIS) Regulation 2018

The Cyber Enforcement Approach is ultimately used by the Cyber Security Team, as the first line enforcement stage for CAP1753 compliance and has been developed in line with the stages of enforcement set out in the various regulatory enforcement approaches described herein.

Where an organisation is failing to meet the requirements of the Cyber Security Oversight Process for Aviation (CAP1753), the Cyber Team will use a structured and proactive approach to encouraging compliance.

Cyber Enforcement Approach steps include:

Identification and Notification: If an organisation is found to be non-compliant, the Cyber Team will formally notify the Accountable Manager, Cyber Security Responsible Manager and/or Security Manager and provide detailed information on the areas of non-compliance.

Corrective Actions: The organisation is required to develop a corrective action plan to address the identified issues. This plan must outline specific steps and timelines for achieving compliance.

Monitoring and Support: The Cyber Team will closely monitor the implementation of the corrective action plan, providing guidance and support as needed to ensure the organisation remains on track.

Reassessment: Once the corrective actions have been implemented, the Cyber Team will conduct a reassessment to verify that the organisation has achieved compliance.

Escalation Action: If an organisation fails to adequately engage, address non-compliance or where a serious non-compliance resulting in an immediate threat to safety, security or resilience, the Cyber Team may take appropriate and proportionate enforcement action in accordance with existing CAA and DfT enforcement approaches.

5. Safety and Airspace Regulation Regulatory Enforcement Approach

The CAA Cyber Team will, in collaboration and consultation with the applicable safety domains and in accordance with the applicable Memorandum of Understanding' between AAA, Flight Operations, Airworthiness, abide by the Safety and Airspace Regulation Enforcement Guidance - CAP 1074[1] to address any breach, or suspected or potential breach, of the safety regulation provisions listed in Annex 1 – Cyber Security Provisions.

The CAA Safety and Airspace Regulation Enforcement Guidance (CAP 1074) aims to provide a clear framework for enforcing safety and airspace regulations within the UK and supports the CAA's broader regulatory enforcement policy, ensuring that all actions taken are proportionate, transparent, and aimed at improving overall aviation safety.

The primary objectives of CAP 1074 are to:

Ensure Compliance: Promote adherence to safety and airspace regulations to maintain high standards in civil aviation.

Enhance Safety: Protect the safety of passengers, crew, and the general public by addressing and mitigating risks.

Fair Enforcement: Apply enforcement actions consistently and fairly across all regulated entities.

Transparency: Offer clear guidance on the enforcement process, including the types of enforcement actions and the circumstances under which they are applied.

The Cyber Team will notify the relevant SARG teams upon the identification of a non-compliance or suspected non-compliance and will work with the teams to fully understand the safety consequences and identify appropriate enforcement action measures.

[1] https://www.caa.co.uk/publication/download/14617

6. Avsec Regulatory Enforcement Approach

For organisations in scope of CAP1753 under the National Aviation Security Programme (NASP), the CAA Cyber Team will use the (National Quality Standards for Civil Aviation Security Programmes) (NQSCP) Stepped Approach to address deficiencies against Chapter 13 of the UK Single Consolidated Direction (SCD).

The NQSCP stepped enforcement approach seeks to ensure continued compliance with aviation security standards through a graduated and proportionate response to deficiencies. Overall, this approach seeks to create a balanced and effective enforcement system that supports the continuous improvement of aviation security.

The primary objectives of this approach include:

Proportional enforcement: Applying enforcement measures that are appropriate to the severity of the non-compliance, ranging from warnings to more stringent actions like prosecution.

Encouraging compliance: Providing guidance and support to help aviation industry stakeholders understand and meet security requirements.

Continuous improvement: Promoting ongoing evaluation and enhancement of security practices to adapt to evolving threats and maintain high security standards.

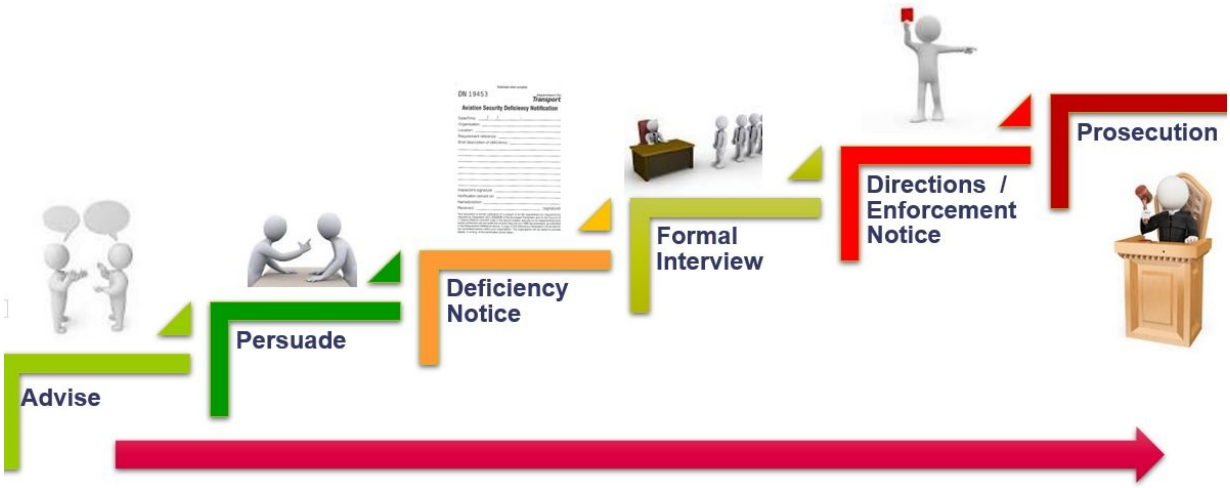

Figure 3: CAA Aviation Security Stepped Enforcement Approach

The Cyber Team will notify the internal and external teams upon the identification of a non-compliance or suspected non-compliance and will work with the teams to fully understand the security consequences and identify appropriate enforcement action measures.

7. DfT's Stepped Enforcement Approach for NIS

As co-competent authorities the DfT and CAA will use a stepped approach to enforcement for the Network and Information Systems Regulation 2018 (NIS) when an Operator of Essential Service (OES) is found to be failing to meet requirements. This relies heavily on a collaborative approach between the DfT, CAA and OES. Any enforcement, particularly the issuing of penalties, will be a last resort and in all cases will be proportionate to the failing identified. The stepped approach can be summarised as follows:

Step 1: Advise and persuade

When any deficiencies are identified, the initial approach taken by the CAA will be to engage and discuss this with the OES using the Cyber Enforcement Approach. This will include discussing what the failing or deficiency is and how and when it can be addressed. The CAA will agree the remedial actions proposed by the OES and when these actions should be completed. The CAA may wish to follow-up with further assessments or audits to ensure that these actions have been taken and any failings have been addressed appropriately and proportionately. More formal communications may be required, if these actions fail to be addressed in the agreed timeframe. The DfT and CAA may issue information notices requiring the OES to provide specified information to support compliance assessment.

Step 2: Enforcement notice

Where the initial informal approach has not worked, and failings are not being addressed, the CAA will escalate to DfT and make a recommendation for enforcement. DfT will determine whether a formal enforcement notice will be issued. A formal enforcement notice will set out the reasons for serving the notice, the failings identified, the steps to be taken and the time-period in which they need to be completed.

Step 3: Penalty notice

Where the OES has failed to take adequate steps within the specified time to rectify a failure identified in an enforcement notice a monetary penalty may be issued. In practice such a step is likely to be taken only in extreme cases and as a last resort where the initial actions taken by the DfT and CAA have not been successful at instigating action by the OES. In determining the value of the monetary penalty, the DfT will consider the appropriate and proportionate level within the prescribed limits.

8. Space

The CAA Space team employs a range of enforcement tools and powers to ensure compliance and deter non-compliance with the Space Industry Regulations 2021. The Spaceflight Enforcement Policy - CAP 2987[2] focuses on ensuring compliance with spaceflight regulations through a balanced and transparent framework that includes a range of enforcement tools and powers, such as monitoring licensees, addressing contraventions, taking proportionate actions including issuing notices, or revoking licences when necessary. Any proposed enforcement will be considered in the context of the CAA's overriding duty to ensure public safety under section 2 of the Space Industry Act 2018[3].

Ultimately the Space Regulatory team are responsible and accountable for undertaking any enforcement action deemed necessary. The CAA Cyber Team will work with the Space Regulatory team upon identification of any non-compliance or suspected non-compliance relating to cyber security requirements and will work collaboratively with the team during the enforcement process.

9. Appeals / Challenge

Where the Civil Aviation Authority (CAA) has made a decision or issued a proposal which affects you, you may be entitled to appeal against it or to ask for a review.

If you wish to appeal against a decision or proposal of the CAA, or if you wish to challenge the conduct staff you can find more details and specific channels depending on the nature of your complaint by visiting the complaints section of the CAA website: Make a report or complaint | UK Civil Aviation Authority

[2] Spaceflight enforcement policy

[3] Space Industry Act 2018