Computer Misuse Act 1990

Call for Information

This Call for Information begins on 11 May 2021.

This Call for Information ends on 8 June 2021.

**About this Call for Information**

|  |  |
| --- | --- |
| **To:** | The scope of this Call for Information is the Computer Misuse Act 1990, including the offences in the Act, and the powers available to law enforcement agencies to investigate those offences. This Call should be read particularly by those interested in the CMA and in the ability of the UK to respond to cyber-dependent threats.  |
| **Duration:** | From 11/05/21 to 08/06/21 |
| **Enquiries (including requests for the paper in an alternative format) to:** | The CMA Review Home Office2 Marsham StreetLondonSW1P 4DFEmail: CMAReview@homeoffice.gov.uk |
| **How to respond:** | Please send your response by 8 June 2021 to:The CMA Review Home Office2 Marsham StreetLondonSW1P 4DFEmail: CMAReview@homeoffice.gov.uk |

Contents

Executive summary 2

The subject of this Call for Information 2

Background 3

Information Sought 5

Context 5

Offences 5

Protections 5

Powers 6

Jurisdiction 6

Sentences 6

General 6

International best practice 6

About you 7

Contact details and how to respond 8

Complaints or comments 8

Extra copies 8

Representative groups 8

Confidentiality 8

Consultation principles 11

# Executive summary

## The subject of this Call for Information

The Computer Misuse Act 1990 (CMA) is now 30 years old, and in general has proved to be a far-sighted piece of legislation which law enforcement are still able to use to prosecute cyber-dependant related crime, despite its age. There have been a number of amendments to the Act, most recently in 2015, to ensure that UK legislation meets the requirements of the Council of Europe Convention on Cybercrime (Budapest Convention) and other relevant EU directives. However, these changes were relatively limited.

As set out in The National Cyber Security Strategy 2016 – 2021 (NCSS), there are two major categories of cybercrime. There are cyber-dependent crimes, such as hacking into computer systems, to view, steal or damage data; and cyber-enabled crimes, which include ‘traditional’ crimes such as cyber-enabled fraud and data theft.

The CMA is the main UK legislation relating to cyber-dependent crime. Our intention with this Call for Information is to identify whether there is activity causing harm in the area covered by the Act that is not adequately covered by the offences. This includes whether law enforcement agencies have the necessary powers to investigate and take action against those attacking computer systems, and whether the legislation is fit for use following the technological advances since the CMA was introduced. In addition, we would welcome any other suggestions on how the response to cyber-dependent crime could be strengthened within the legislative context. This Call for Information does not cover cyber-enabled crime.

# Background

This paper sets out the Call for Information on the Computer Misuse Act 1990. The consultation is aimed at academia, business, law enforcement agencies, the cybersecurity industry and the private sector in the United Kingdom.

The Government’s Integrated Review of Security, Defence, Development and Foreign Policy committed the UK to fortifying its position as a world-leading and responsible cyber power, taking a new comprehensive approach to the UK’s cyber capability.

The Government will publish the UK’s new cyber strategy in 2021. Under this strategy, our priority actions will be:

* To strengthen the UK’s cyber ecosystem, enabling a whole-of-society approach to cyber and deepening the partnership between government, academia and industry.
* To build a resilient and prosperous digital UK, where citizens feel safe online and confident that their data is protected.
* To take the lead in the technologies vital to cyber power, building our industrial capability where necessary and ensuring the UK can adopt emerging technologies securely.
* To promote a free, open, peaceful and secure cyberspace, working with other governments and industry, and drawing on the UK’s thought leadership in cyber security.
* To detect, disrupt and deter our adversaries.

The Computer Misuse Act 1990 supports these objectives, particularly the final strand, by providing law enforcement and prosecutorial agencies with the ability to prosecute those who commit cyber-dependent offences. It forms a key part of our approach to deterring such attacks.

However, the Act was passed 30 years ago, and since then the reliance of society on the digital world has increased enormously, we are now critically dependent on the internet. The threat is significant. As the Serious Organised Crime Strategy 2018 sets out, cyber security breaches create significant costs for businesses, particularly ransomware attacks, where businesses and organisations, including the NHS, are significantly disrupted. To take action against these threats, the Government has invested £1.9bn through the National Cyber Security Programme between 2016 – 2021 to develop the UK’s cybersecurity.

It is absolutely essential that the UK has the right legislation and powers in place to allow action to be taken. Therefore the Government believes that now is the right time to seek the views of stakeholders on whether there are legislative gaps in our response to cyber-dependent crime, and in particular if there is a need to make changes to the Computer Misuse Act to improve our ability to protect our society from the threat posed by cyber-dependent crime.

# Information Sought

The Call for information seeks the views of respondents on the following areas

- Context

- Offences

- Protections

- Powers

- Jurisdiction

- Sentences

- International comparisons

We welcome suggestions on all of these, and also an indication of the benefits and risks that would accrue from any changes.

## Context

**Q1. How would you describe the understanding that your organisation/business has of the Computer Misuse Act?**

**Q2. How does your organisation use the CMA, or how is it affected by it?**

## Offences

**Q3. Do the offences set out in the CMA adequately cover cyber-dependent harms?**

**Q4. Are there any gaps in the legislation, and if so, what are they?**

**Q5. What are the potential future areas where the CMA may not adequately cover the harms?**

**Q6. What changes could we make now to meet those challenges?**

## Protections

**Q7. Do the protections in the CMA for legitimate cyber security activity provide adequate cover?**

**Q7b. If not, what changes would you wish to see made?**

**Q9. What risks do you see from any changes to protections?**

## Powers

**Q10. Do you believe that law enforcement agencies have adequate powers to tackle cybercrime?**

**Q11. Do you think the CMA should include any new powers (such as providing law enforcement agencies with powers to seize domain and IP seizure from criminals or criminalising data commoditisation)?**

## Jurisdiction

**Q12. Does the CMA provide adequate criminalisation of offences under the Act carried out against the UK from overseas?**

**Q12b. If not, what changes would you like to see made?**

## Sentences

**Q13. Do you believe that the sentences relating to the offences in the CMA are adequate?**

**Q13b. If not, how would you see sentencing guidelines changed in proportion to the harms these offences cause?**

## General

**Q14. Are there any other areas where you believe improvements to legislation could be made to enhance our response to cyber-dependent threats?**

**Q15. Are there are opportunities for improvements to the UK response to the threat from criminals operating online now we have greater flexibility to set our own laws outside of the European Union'?**

## International best practice

**Q16. Are there examples of legislation in other countries that the UK should consider?**

**Q17. If so, how has this legislation empowered governments to better investigate and prosecute cyber-dependent crimes?**

**Thank you for participating in this consultation**

# About you

Please use this section to tell us about yourself

|  |  |
| --- | --- |
| **Full name** |  |
| **Job title** or capacity in which you are responding to this consultation exercise (for example, member of the public) |  |
| **Date** |  |
| **Company name/organisation** (if applicable) |  |
| **Address** |  |
|  |  |
| **Postcode** |  |
| If you would like us to acknowledge receipt of your response, please tick this box | [ ] (please tick box) |
| Address to which the acknowledgement should be sent, if different from above |  |
|  |
|  |

**If you are a representative of a group**, please tell us the name of the group and give a summary of the people or organisations that you represent.

|  |
| --- |
|  |
|  |
|  |
|  |

# Contact details and how to respond

Please send your response by 8 June 2021 to:

The CMA Review
Home Office

2 Marsham Street

London

SW1P 4DF

Email: CMAReview@homeoffice.gov.uk

## Complaints or comments

If you have any complaints or comments about the Call for Information process you should contact the Home Office at the above address.

## Extra copies

Further paper copies of this consultation can be obtained from this address and it is also available online at https://www.gov.uk/search/policy-papers-and-consultations.

Alternative format versions of this publication can be requested from CMAReview@homeoffice.gov.uk.

## Representative groups

Representative groups are asked to give a summary of the people and organisations they represent when they respond.

## Confidentiality

Information provided in response to this Call for Information, including personal information, may be published or disclosed in accordance with the Freedom of Information Act 2000 (FOIA). If you want the information that you provide to be treated as confidential, please be aware that, under the FOIA, there is a statutory Code of Practice with which public authorities must comply and which deals, among other things, with obligations of confidentiality.

In view of this it would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information, we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding.

# Consultation principles

The principles that government departments and other public bodies should adopt for engaging stakeholders when developing policy and legislation are set out in the consultation principles.

<https://www.gov.uk/government/publications/consultation-principles-guidance>



© Crown copyright 2021

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit [nationalarchives.gov.uk/doc/open-government-licence/version/3](http://nationalarchives.gov.uk/doc/open-government-licence/version/3/)

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at <https://www.gov.uk/search/policy-papers-and-consultations>

Any enquiries regarding this publication should be sent to us at CMAReview@homeoffice.gov.uk.