Home Office

Digital, Data and Technology
Home Office Cyber Security
Lunar House
Croydon
CR9 2BY
www.homeoffice.gov.uk

Ryan Jarvis
Via email: request-926188-52f116f4@whatdotheyknow.com

28 December 2022

Dear Ryan Jarvis,

Freedom of Information Act 2000 Request (Our Reference 73275)

Thank you for your email of 05 December 2022 in which you ask for information regarding the Home Office's use of the '@homeoffice.gov.uk' domain. A full copy of your request can be found in **Annex A**. Your request has been handled as a request for information under the Freedom of Information Act 2000 (FOIA).

For Question 1, we neither confirm or deny whether we hold the information that you have requested. Sections 24 (National Security) and 31 (Law Enforcement) of the FOI Act absolve us from the requirement to say whether or not we hold information, if its disclosure could undermine departmental responsibilities for national security and/or law enforcement, and the public interest falls in favour of neither confirming or denying.

Sections 24 and 31 of the Act are qualified exemptions and requires consideration of the public interest test. An explanation of the public interest test is set out in **Annex B**.

This response should not be taken as evidence that the information you have requested is or is not held by the Home Office.

For Questions 2 and 3, I can confirm that the Home Office holds the information that you have requested. However, after careful consideration we have decided that the information is exempt from disclosure under sections 24 (National Security) and section 31 (Law Enforcement). These are both qualified exemptions, which means that the balance of the public interest in applying them must be considered. Arguments for and against disclosure, in terms of the public interest are set out in the **Annex C**.

If you are dissatisfied with this response you may request an independent internal review of our handling of your request by submitting a complaint within two months to foirequests@homeoffice.gov.uk, quoting reference **73275**. If you ask for an internal review, it would be helpful if you could say why you are dissatisfied with the response.

As part of any internal review the Department's handling of your information request would be reassessed by staff who were not involved in providing you with this response. If you were to remain dissatisfied after an internal review, you would have a right of complaint to the Information Commissioner as established by section 50 of the FOIA.

A link to the Home Office Information Rights Privacy Notice can be found in the following link. This explains how we process your personal information: https://www.gov.uk/government/publications/information-rights-privacy-notice.

Yours sincerely,

Home Office Cyber Security
Email foirequests@homeoffice.gov.uk

Annex A

From: Ryan Jarvis request-926188-52f116f4@whatdotheyknow.com
Sent: 05 December 2022 07:07
To: FOI Requests FOIRequests@homeoffice.gov.uk
Subject: Freedom of Information request - Home Office Email Security & Classifications Policies

Dear Home Office,

I am writing to respectfully make a formal request in accordance with the Freedom of Information Act 2000.

The privacy of emails sent via the @homeoffice.gov.uk domain is at risk. This domain does not appear to have MTA-STS configured. This means that email privacy (using TLS) is vulnerable to downgrade, allowing an attacker to read the contents of emails.

My request is as follows:-

1. Please can the department confirm why it has opted not to use MTA-STS as a potential CySec safeguard when communicating via email on the @homeoffice.gov.uk domain name?

2. Please can the department provide disclosure of its email security classifications policy.

3. Please can the department provide disclosure of the number of security incident reports made internally and/or externally which relate to concerns surrounding email security.

If I am able to provide any further information in support of this request, please do not hesitate to contact me.

Yours faithfully,

Ryan Jarvis

Annex B - Freedom of Information request from Ryan Jarvis (73275)

Information Requested

1. Please can the department confirm why it has opted not to use MTA-STS as a potential CySec safeguard when communicating via email on the @homeoffice.gov.uk domain name?

Response

The Home Office neither confirms nor denies whether information relevant to your request. In considering our response to your request, we have considered the exemption provisions of sections 24 (National Security) and 31 (Law Enforcement) of the Act:

Section 24(2) (National Security)

> (2) The duty to confirm or deny does not arise if, or to the extent that, exemption from section 1(1)(a) is required for the purpose of safeguarding national security

Section 31(3) (Law enforcement)

> (3) The duty to confirm or deny does not arise if, or to the extent that, compliance with section 1(1)(a) would, or would be likely to, prejudice any of the matters mentioned in subsection (1).

Public interest test considerations

Some of the exemptions in the FOI Act, referred to as 'qualified exemptions', are subject to a public interest test (PIT). This test is used to balance the public interest in disclosure against the public interest in favour of withholding the information, or the considerations for and against the requirement to say whether the information requested is held or not. We must carry out a PIT where we are considering using any of the qualified exemptions in response to a request for information.

The 'public interest' is not the same as what interests the public. In carrying out a PIT we consider the greater good or benefit to the community if the information is released or not. The 'right to know' must be balanced against the need to enable effective government and to serve the best interests of the public.

The FOI Act is 'applicant blind'. This means that we cannot, and do not, ask about the motives of anyone who asks for information. In providing a response to one person, we are expressing a willingness to provide the same response to anyone, including those who might represent a threat to the UK.

Considerations in favour of confirming whether or not we hold the information

We acknowledge the public interest in openness and transparency and we recognise that to confirm or deny details would indicate the use of specific technologies in operation at the Home Office. Transparency in this matter would enhance the public's knowledge of systems and processes in place, and to some limiting degree, how public money and resource is used.

Considerations in favour of neither confirming nor denying whether we hold the information

Section 24 – National Security:

To confirm or deny would not be in the interest of the UK's national security. It is considered that, to provide details on whether or not the Home Office has opted not to use MTA-STS, would provide useful information to those who might seek to commit crime by allowing them to potentially hack into and attack Home Office IT systems – this is clearly not in the public interest. Furthermore, to confirm or deny would also undermine the Home Office's key role in the infrastructure of the UK and its ability to safeguard national security. There is clearly a strong public interest in doing everything we can to detect and prevent crime and protect the public at large.

Section 31 – Law Enforcement:

To confirm or deny would not be in the interest of the UK's Law Enforcement capabilities. It is considered that, to provide details on whether or not the Home Office has opted not to use MTA-STS, would expose the Home Office to potential threats of a criminal nature. By confirming details of this one way or the other, it puts firm knowledge into the public domain which could prejudice the prevention or detection of crime, the apprehension or prosecution of offenders, the administration of justice, the operation of immigration controls and the purpose of ascertaining whether any person has failed to comply with the law.

Conclusion

We conclude that the balance of the public interest lies in neither confirming nor denying whether we hold the information. This response should not be taken as confirmation that the information you have requested is or is not held by the Home Office.

Annex C - Freedom of Information request from Ryan Jarvis (73275)

Information Requested

2. Please can the department provide disclosure of its email security classifications policy.

3. Please can the department provide disclosure of the number of security incident reports made internally and/or externally which relate to concerns surrounding email security.

Response

Section 24(1) – provides that information which does not fall within subsection 23(1) is exempt from disclosure if exemption from section 1(1) (b) is required for the purpose of safeguarding national security.

Section 31(1)(a) – provides that information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice the prevention or detection of crime.

Public interest test considerations

Some of the exemptions in the FOI Act, referred to as 'qualified exemptions', are subject to a public interest test (PIT). This test is used to balance the public interest in disclosure against the public interest in favour of withholding the information, or the considerations for and against the requirement to say whether the information requested is held or not. We must carry out a PIT where we are considering using any of the qualified exemptions in response to a request for information.

The 'public interest' is not the same as what interests the public. In carrying out a PIT we consider the greater good or benefit to the community as a whole if the information is released or not. Transparency and the 'right to know' must be balanced against the need to enable effective government and to serve the best interests of the public.

The FOI Act is 'applicant blind'. This means that we cannot, and do not, ask about the motives of anyone who asks for information. In providing a response to one person, we are expressing a willingness to provide the same response to anyone, including those who might represent a threat to the UK.

Considerations in favour of disclosing the information

The release of this information would indicate the types of email security classifications adhered too within the policy which would prevent any safeguarding said policy enables. Furthermore, sharing the numbers of security incident reports made internally and/or externally surrounding email security would allow for vulnerabilities against any attacks. Transparency in this matter would enhance the publics knowledge of information access attempts by staff in the legitimate work of the Home Office but are considered unsuitable. This request would disclose our effectiveness at enabling secure email communications and detecting and monitoring any associated security incident reporting.

Considerations in favour of maintaining the exemption

Confirming what information is held could assist someone in determining the information held within emails via the classification's identification. As well as scoping out the number of security related incident reports which would outline the Home Office's vulnerability to potential attacks. Although the Home Office is just one department, it is important to consider the broader picture, because if the same (or similar) information was revealed by other key public authorities, a UK-wide picture could be built-up of potential vulnerabilities and therefore a more detailed understanding of the attack surface across Government.

Section 24(1) – National Security

Disclosure of information would not be in the interest of the UK's national security. It is considered that to provide these details on the policies and controls around email security classifications, and relative success, would provide useful information to those who might seek to commit crime by targeting Home Office employees via email contents. This is clearly not in the public interest and would not be in the interest of the UK's national security and hence why section 24 applies.

Section 31(1) – Law Enforcement

If the Home Office (or any authority) released information, detailing the number of security incident reports made internally and/or externally which relate to concerns surrounding email security, a criminal could deduce with the email classifications policy (if released) which rules are being used to classify certain information and indicate targeting of email contents. Releasing information which would allow malicious actors to potentially evade detection or arrest is not considered in the public interest, and hence the additional application of section 31.

In summary disclosure of this information would undermine the Home Office's key role in the infrastructure of the UK and its ability to safeguard national security. There is clearly a strong public interest in doing everything we can to detect and prevent crime and protect the public at large. It is considered that disclosure of the requested information would prejudice both the prevention of crime and national security.

Conclusion

Disclosure under the FOIA is a release to the public at large and the safety of the public and protection of national security, together with effective law enforcement, is of paramount importance and for the reasons outlined above, outweigh the public interest factors in favour of disclosure.