OFFICE OF THE
IMMIGRATION SERVICES
COMMISSIONER

OISC

Freedom of Information Request

FOI/AH/17/16

DETAILS RELATING TO IT SECURITY OF OISC

30 May 2017

Dear Sir/Madam

I am writing to submit a Freedom of Information request regarding computing services at your facility. Could you please answer for me the following, where applicable in the time span of the last 5 years:

1. Have there been any security events related to the computer systems at the facility?
2. If so, could you please provide a short narrative of the event and the actions taken as well as, if possible, any diagnostic information that resulted from it, such as computer reports or official reports.
3. Could you please provide me with a copy of your in-house cyber-security information. This could be, but is not limited to, power point presentations, posters or internal PDF documents.
4. Could you please, if possible, confirm the specification of systems currently operating at your facility? I would also request ny technical specification type reports that may be available.

If this information is held elsewhere, I remind you of your obligation under section 16 of the Freedom of Information act, which details your duty to aid me in my request and, if necessary to help me reframe the question to obtain the information I seek.
Despite the fact that I, as a requester, do not have to show that releasing the information is in the public interest (as opposed to withholding it being in the public interest), I suggest that releasing the information is indeed in the public interest. This is because of general public interest in transparency. It also is in the public interest because, as the facilities in question are a publicly funded body, there is a significant interest in the means with which public money is used by them. There is also a public interest in people knowing about any risks to which they have been exposed by information security events. Moreover, the public has a right to know about the existence of these events. Their knowledge may help them take steps to protect themselves. Or, conversely, if the information security events pose no risk to safety, there is a public interest in knowing that fact, as it may reassure the public that appropriate steps are taken to secure sensitive information, or remedy any deficiencies in the information security regimes in place. Moreover, it there is no risk to public safety, there is little prospect of it being in the public interest to withold the information.

Yours sincerely,

RESPONSE

23 June 2017

Dear [REDACTED],

I am the OISC's Information Officer and it is my responsibility to reply to enquiries such as yours.

You have requested the Commissioner to provide you with the following information:

1. Have there been any security events related to the computer systems at the facility?
2. If so, could you please provide a short narrative of the event and the actions taken as well as, if possible, any diagnostic information that resulted from it, such as computer reports or official reports.
3. Could you please provide me with a copy of your in-house cyber-security information. This could be, but is not limited to, power point presentations, posters or internal PDF documents.
4. Could you please, if possible, confirm the specification of systems currently operating at your facility? I would also request any technical specification type reports that may be available.

On 6 June 2017 I acknowledged this request and sought clarification from you, over the meaning of 'security events'. In a response dated 8 June 2017, you clarified that you were 'interested in cyber-security incidents which have occurred within the last 5 years'.

I have carefully considered your request and have decided to exempt all of the requested information under Section 31(1)(a) of the Freedom of Information Act 2000 because I have concluded that disclosure would prejudice the prevention or detection of crime.

The Commissioner is unable to provide any information relating to cyber-security incidents because disclosure of this information could assist individuals in establishing whether certain cyber attacks have been detected. Disclosure would also provide individuals with a valuable insight into the OISC's level of resilience, thereby facilitating the commissioning or concealment of crime in relation to information held by the OISC.

The Commissioner is also unable to disclose information relating to its cyber security system, specification of systems or specification reports because such information would provide individuals with valuable insight into the OISC's security procedure, its level of resilience and its perceived strengths and weaknesses. For example, it would make it easier for attackers to determine what kind of defensive measures were in place, where the OISC's weaknesses might be and the likely identity of contractors working in or with the OISC. Disclosure of this information could also assist external parties in attempting a cyber-attack/hack into the OISC's IT infrastructure.

As this is a qualified exemption I am required to apply the public interest test. I have carefully considered the public interest arguments put forward, namely, that full disclosure would make the public better informed how public bodies secure data and also that public bodies should be accountable for their expenditure and allocation of funds. However, in my view, disclosure of this information could allow individuals to illegally access the OISC's IT systems and cause them to fail and enable them to have access to sensitive information stored within them. Therefore, I have decided to maintain my decision to exempt all of the requested information.

If you are dissatisfied with the handling of your request, you have the right to ask for an internal review. Internal review requests should be submitted within two months of the date of

receipt of the response to your original request. Please quote the above reference number in any request for an internal review.

If you are not content with the outcome of the internal review, you have the right to apply directly to the Information Commissioner for a decision. Details on how to do this are on his website at http://ico.org.uk/.

Kind regards,

For and on behalf of the Office of the Immigration Services Commissioner