The Crown Estate Disclosure Log

Case no: 1166
Date received: 5 February 2020
Subject: Cybersecurity
Request response
1. Does your organisation have a formal policy regarding the production of information and or cyber security risk assessments? Yes *a. If yes, please can you provide a copy of the above policy?* No - we are unable to provide you with a copy because the exemption at section 31(1)(a) FOIA applies as the information it contains would help someone breach our systems. A further explanation of this exemption and the public interest test that relates to it can be found in the annex to this email. *2. Does your organisation hold a register of Information and/or cyber security risk (outside that of the corporate risk register)* Yes *a. Please can you list the top ten Information and/or Cyber Security Risks?* *b. How many risks are there in total on the register?* *c. Please state how many risks would be categorised as the highest risk level (i.e. Critical)?* *d. Please state how many risks would be categorised as the second highest risk level (i.e. Critical)?* *e. Please state how many risks would be categorised as the third highest risk level (i.e. Critical)?* *f. How many risk levels do you have in total (i.e. 5)?* Again, we hold the information listed at points a to f but we are unable to disclose them as the exemption at 31(1)(a) FOIA is engaged. *3. Do any of the identified information and or cyber security risks also exist on the corporate risk register?* Yes

a. If yes, what are those risks?

We hold this information but are unable to disclose it as the exemption at 31(1)(a) FOIA is engaged.

4. When undertaking an information / cyber security risk assessment, does the authority follow a structured risk assessment process?
Yes

a. If so, what is that process?
We hold this information but are unable to disclose it as the exemption at 31(1)(a) FOIA is engaged.

5. Does your organisation follow ISO31000 when undertaking an information / cyber security risk assessment?
Yes

6. Does your organisation hold ISO27000 accreditation?
Yes

7. Does your organisation have a policy of adhering to any information security standard or framework (i.e. ISO27000, NIST etc)?
Yes

a. If yes, please provide a copy of the above policy?
We hold this information but are unable to disclose it as the exemption at 31(1)(a) FOIA is engaged.

8. Does the authority have the following roles within the origination:
a. Chief Security Officer (CSO),

i. If yes, which role does the CSO report into?

b. Chief Information Security Officer (CISO)

i. If yes, which role does the CISO report into?

c. Head of Information Security (Hd InfoSec)

i. If yes, which role does the Hd InfoSec report into?
We do not have these job titles at our organisation, but their functions are carried out in other roles.

9. Who within your organisation who is accountable for undertaking information / cyber security risk assessments (i.e. Chief Information Security Officer, Head of Information Security, Head of Information Technology)?

10. Who within the authority is responsible for undertaking information / cyber security risk assessments (i.e. Chief Information Security Officer, Head of Information Security, Head of Information Technology)?

11. How many people within the organisation are responsible for undertaking information / cyber security risk assessments?

12. Does the person(s) responsible for undertaking information / cyber security risk assessment:

a. Have any formal training in this regard?

i. If so, what was it?

b. Have any industry qualifications/certification in this regard?

i. If so, what are they?
We hold the information requested but are unable to disclose it as the exemption at 31(1)(a) FOIA is engaged.

13. How many people (permanent and contractors) currently work for the authority?
530

14. How many people (permanent and contractors) currently work for the authority in information technology roles?
58

15. How many people (permanent and contractors) currently work for the authority in information / cyber security roles?
We hold this information but are unable to disclose it as the exemption at 31(1)(a) FOIA is engaged.

I hope that this response is helpful. However, if you are not satisfied with the way we have handled your information request, you may appeal our decision which will then be investigated through an internal review. If you are not content with the outcome of that, you have the right to refer any complaint directly to the Information Commissioner's Office (ICO) (contact details are available at: www.ico.org.uk). The ICO will usually expect you to have first exhausted our own complaints procedure before raising any concerns with them.

Annex - Section 31(1)(a) Public Interest Test

We are unable to provide you with some of the information you have requested because it is exempt from disclosure under section 31(1)(a) FOIA. Section 31(1 (a) exempts information if its disclosure is likely to prejudice the prevention or detection of crime. This relates to the information you have requested which would reveal our organisational processes in relation to cyber security.

Section 31 is a qualified exemption and we are required to conduct a public interest test when applying any qualified exemption. This means that after it has been decided that the exemption is engaged, the public interest in releasing the information must be considered. If the public interest in disclosing the information outweighs the public interest in withholding it then the exemption does not apply and the information must be released. In FOIA there is a presumption that information should be released unless there are compelling reasons to withhold it.

In this case, we have concluded that the balance of the public interest is in favour of withholding information covered by the section 31(1)(a) exemption. Considerations in favour of the release of the information included the principle that there is a public interest in transparency and accountability in disclosing information about our procedures as a public body. However, release of this information would make The Crown Estate more vulnerable to crime, such as a malicious attack on its computer systems, and the disclosure of the information you have requested could therefore facilitate a criminal offence. As a result, in this case the public interest weighs in favour of non-disclosure.