

Keeping People Safe



FREEDOM OF INFORMATION REQUEST



Request Number: F-2020-01956

Keyword: Organisational Information/Governance

Subject: Cyber Security

Request and Answer:

In relation to request no 1, 2, 3, 4, 5 and 7 Police Service of Northern Ireland is providing an NCND response and will explain this further in the response below. Additionally in respect of Request 6 PSNI is exempting this request under Section 40 as detailed under:

Request 1

What SEIM (Security Event and Incident Management) solution is used by your organisation?

Request 2

When does your SEIM (Security Event and Incident Management) platform license subscription come up for renewal?

Request 3

If the SEIM (Security Event and Incident Management) solution was purchased via third party please disclose the contracting party's details?

Request 4

Do you outsource your security management to a third party (managed security service provider)? If so can you disclose the name of the managed security service provider.

Request 5

When does the current service contract from the current managed security service provider end?

Request 7

How many cyber security breaches has your organisation had over the past 2 yrs?

Answer

In accordance with the Act, this letter represents a Refusal Notice for this particular request. The Police Service of Northern Ireland can neither confirm nor deny that it holds the information you have requested.

Section 1 of the Freedom of Information Act 2000 (FOIA) places two duties on public authorities. Unless exemptions apply, the first duty at Section 1(1)(a) is to confirm or deny whether the information specified in the request is held. The second duty at Section 1(1)(b) is to disclose

information that has been confirmed as being held.

Where exemptions are relied upon Section 17(1) of FOIA requires that we provide the applicant with a notice which

- a) states that fact,
- b) specifies the exemption(s) in question and
- c) states (if that would not otherwise be apparent) why the exemption applies.

The Police Service of Northern Ireland (PSNI) can Neither Confirm Nor Deny that it holds the information relevant to your request as the duty in Section 1(1)(a) of the Freedom of Information Act 2000 does not apply by virtue of the following exemptions:

Section 24(2) National Security: 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: 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).

The full text of exemptions can be found at www.legislation.gov.uk and further guidance on how they operate can be located on the Information Commissioners Office website www.ico.org.uk.

Section 24 is a qualified prejudice based exemption and evidence of harm and a public interest test must be conducted.

Section 31 is a qualified prejudice based exemption and evidence of harm and a public interest test must be conducted.

'Neither Confirm nor Deny' (NCND)

There may be occasions when complying with the duty to confirm or deny under section 1(1) (a) would in itself disclose sensitive or potentially damaging information that falls under an exemption. In these circumstances, the Act allows a public authority to respond by refusing to confirm or deny whether it holds the requested information.

The decision to issue a 'neither confirm nor deny' response is not affected by whether we do or do not hold the information but relates to the consequences of confirming or denying the information is held. The starting point and main focus in most cases will be theoretical considerations about the consequences of confirming or denying that a particular type of information is held. The decision to neither confirm nor deny is separate from a decision not to disclose information and needs to be taken entirely on its own merits.

PSNI follow the Information Commissioner's Guidance in relation to 'NCND' and you may find it helpful to refer to this at the following link:

[https://ico.org.uk/media/for-organisations/documents/1166/when to refuse to confirm or deny section 1 foia.pdf](https://ico.org.uk/media/for-organisations/documents/1166/when_to_refuse_to_confirm_or_deny_section_1_foia.pdf)

Harm

The release of any information about PSNI's ICT infrastructure (especially including specific details of a SIEM product) presents a real, immediate and significant risk of harm. It could reveal potential security weaknesses, operating procedures, capability and methodology therefore increasing our vulnerability to a malicious attack. PSNI's systems may rightly be viewed as a rich target for criminal or terrorist organisations/hacktivists both now and in the future. Recent risk assessments, both at local and national level, prove the likelihood of an attack against corporate networks is on the increase. The potential impact of an attack may negatively impact upon public confidence, damage

the PSNI's reputation, impede or jeopardise investigations, facilitate crime, result in significant financial loss or penalties, or ultimately result in loss of life, e.g. an outage to the 999 service or Command & Control system.

Furthermore, disclosing such information may provide vital pointers which would help anyone with malicious intent to mount a cyber-attack against PSNI's IT systems. The release of such information could act as an incentive for an attack against the Police Service or its suppliers and would increase the potential for compromise of the policing infrastructure. It is well known and well documented that many cyber-attacks are successful when perpetrated against a supplier or sub-contractor of the intended target organisation.

Additionally naming any supplier to the PSNI may increase the risk to that supplier and its staff. The current SEVERE threat in NI applies to Police officers, Police staff and suppliers working on PSNI contracts.

Public Interest Test

Factors favouring Confirming or Denying for Section 24

The information, if held only relates to national security and confirming or denying whether it is held would not actually harm it. The public are entitled to know what public funds are spent on and what security measures are in place, and by confirming or denying the information requested would lead to a better informed public.

Factors against Confirming or Denying for Section 24

By confirming or denying whether any information is held could render the protection of PSNI ICT infrastructure less effective. Protection of the ICT infrastructure of the PSNI is paramount and confirming or denying the information requested could have consequences not just for the protection of PSNI ICT infrastructure but for national security of the UK with an increase in the risk of harm to the public.

Factors favouring Neither Confirming or Denying for Section 31

Confirming or denying whether the information requested is held would provide an insight into the ICT infrastructure of the PSNI. This would enable the public to have a better understanding of the effectiveness of how the PSNI protects its ICT infrastructure. It would greatly assist in the quality and accuracy of public debate. Where public funds are being spent, there is a public interest in accountability and justifying the use of public money.

Factors against Confirming or Denying for Section 31

Confirming or denying that any information is held would have the effect of compromising law enforcement tactics and would also hinder any future investigations. It has been recorded that FOIA releases are monitored by criminals and terrorists and so to confirm or deny information is held concerning PSNI ICT infrastructure would lead to law enforcement being undermined. By confirming or denying that the information you seek exists would hinder the prevention or detection of crime.

However, this should not be taken as conclusive evidence that the information you requested exists or does not exist.

Request 6

Can you provide the email address of the individual that is responsible for your IT Security?

Answer

Section 17(1) of the Freedom of Information Act 2000 requires the Police Service of Northern Ireland, when refusing to provide such information (because the information is exempt) to provide you the applicant with a notice which:

(a) states that fact,

- (b) specifies the exemption in question and
- (c) states (if not otherwise apparent) why the exemption applies.

The exemption/s, as well as the factors the Department considered when deciding where the public interest lies, are listed below:

Section 40(2)(a)(b) by virtue of Section 40(3)(A)(a) – Personal Information - Information constitutes personal data and disclosure would contravene any of the Data Protection principles.

Section 40 is an absolute class based exemption and no public interest test is required.

Section 40 – Personal Information

Section 40 (2) of the FOIA is an absolute exemption which means there is no requirement on PSNI to consider whether there is a public interest in disclosure. It is an interface exemption and we must consider whether release of the information would breach the General Data Protection Regulations ('GDPR') or the Data Protection Act 2018 ('DPA') Third party personal information constitutes 'personal data' under the GDPR (Article 4) and DPA (Part 1 s.3).

Under the Freedom of Information Act, PSNI must consider if information can be released into the public domain. I have therefore considered whether the disclosure of this personal data is subject to the exemption at Section 40(2) of the Freedom of Information Act 2000 by virtue of s40 (3)(A)(a). As this information is 'personal data', PSNI considered whether disclosure would contravene any of the six data protection principles contained within the GDPR or DPA.

The six data protection principles are good information handling standards which PSNI must comply with in relation to how it handles personal information, including deciding whether to disclose it or not. In particular, the first principle requires personal data to be processed in a lawful and fair manner. In considering whether it is 'fair' to any individual to release information about them, PSNI considered the likely expectations of those individuals and the nature of the information involved. Individuals must have confidence that their information is treated sensitively and appropriately by PSNI. We consider those individuals would not have any reasonable expectation PSNI would disclose such information of this nature about them. We consider it would be extremely unfair to those individuals and therefore a breach of the first principle of data protection legislation. This information is therefore exempt under section 40 (2) of the FOIA as it contravenes data protection legislation to release it and PSNI has made the decision to withhold that information.

If you have any queries regarding your request or the decision please do not hesitate to contact me on 028 9070 0164. When contacting the Corporate Information Branch, please quote the reference number listed at the beginning of this letter.

If you are dissatisfied in any way with the handling of your request, you have the right to request a review. You should do this as soon as possible or in any case within two months of the date of issue of this letter. In the event that you require a review to be undertaken, you can do so by writing to the Head of Corporate Information Branch, PSNI Headquarters, 65 Knock Road, Belfast, BT5 6LE or by emailing foi@psni.pnn.police.uk.

If following an internal review, carried out by an independent decision maker, you were to remain dissatisfied in any way with the handling of the request you may make a complaint, under Section 50 of the Freedom of Information Act, to the Information Commissioner's Office and ask that they investigate whether the PSNI has complied with the terms of the Freedom of Information Act. You can write to the Information Commissioner at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. In most circumstances the Information Commissioner will not investigate a complaint unless an internal review procedure has been carried out, however

the Commissioner has the option to investigate the matter at his discretion.

Please be advised that PSNI replies under Freedom of Information may be released into the public domain via our website @ www.psni.police.uk

Personal details in respect of your request have, where applicable, been removed to protect confidentiality.