Keeping People Safe

FREEDOM OF INFORMATION REQUEST

Request Number: F-2020-01087

Keyword: Crime

Subject: Cybercrime

Request and Answer:

Your request for information has now been considered. In respect of Section 1(1)(a) of the Act I can confirm that the Police Service of Northern Ireland does hold some information to which your request relates and this is being provided to you. We further consider the information you seek in request numbers 5 -10 is exempt by virtue of section 31(1)(a)(b) of FOIA and have detailed our rationale as to why this exemption applies. We have also provided you with links to guidance issued by the Information Commissioner's Office which we have followed in responding to your request.

Request 1
Do you have a specialist unit dedicated to cybercrime – which includes computer misuse, cyber enabled and cyber dependent crime?

Answer
Yes, However Cybercrime do not investigate cyber enabled crime, these investigations are dealt with on a case by case basis as per case allocation policy. Cyber Investigations offer assistance/advice to officers who are investigating cyber enabled crime.

Request 2
If so, when did it come into force?

Answer
An investigative team joined the PSNI's e-Crime Unit around April 2015 and shortly after the overall team was re-named as Cyber Crime.

Request 3
What is that unit called?

Answer
The investigative team are referred to as Cyber Crime/Cyber Investigation.

Request 4
The following questions relate to the Unit noted above and specialist officers within that Unit. Please provide information to the requests for information below for the years 2016-2019 indicating your response for each year. Please also indicate in your responses, the numbers of officers or civilians who may also be employed by or working with a Regional Organised Crime Unit, whether by

way of secondment or assignment (or equivalent) specifying which ROCU:

How many police officers or civilians does that unit employ (full time equivalents)?

Answer

YEARS	POLICE OFFICERS (FTE)	POLICE STAFF (FTE)
2016	**19**	**0.75**
2017	**26**	**0.75**
2018	**29**	**0.07**
2019	**30**	**0.07**

Request 5
How many of those are digital forensic or computer specialists?

Request 6
How many civilian investigators does that unit employ (full-time equivalents)?

Request 7
If you do not have a specialist cybercrime unit dedicated to computer misuse and cyber enabled crime, how many specially trained police officers are specifically dedicated to cybercrime investigations (full-time equivalents)?

Request 8
If you do not have a specialist cybercrime unit dedicated to computer misuse and cyber enabled crime, how many specially trained civilians are specifically dedicated to cybercrime investigations (full-time equivalents)?

Request 9
If you do have a specialist cyber-crime unit, how many police officers or civilian staff are dedicated to online fraud or computer enabled economic crime.

Request 10
How many specially trained police officers or civilians dedicated to cyber-crime investigations are also dedicated to online fraud or computer enabled economic crime investigations (full-time equivalents)?

In respect of requests 5-10 this information is exempt and the rationale for withholding this is outlined below:

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 31(1)(a)(b) – Law Enforcement – the prevention or detection of crime and the apprehension or prosecution of offenders.

Section 31 is a prejudice based qualified exemption and there is a requirement to articulate the harm that would be caused in releasing the requested information as well as considering the public interest to ensure that withholding the information is the appropriate response.

Harm
The release of further information relating to Cybercrime units may be harmful to disclose as its release may compromise the effective deployment and disclosure of tactics. This would have a direct impact on crime in certain areas which would ultimately be damaging to law enforcement.

Factors Favouring Disclosure
Releasing this information would better inform the public, demonstrating openness, transparency and accountability on the part of the PSNI.

Factors Against Disclosure
The release of information which could reveal details on the effectiveness of policing operations, taken on its own or together with other information, either already available or the subject of further requests, could damage the law enforcement capabilities of the PSNI.

Decision
PSNI is tasked with the prevention and detection of crime and protecting the public. It has been determined that to disclose the requested information into the public domain would not be in the public interest at this time. For the reasons outlined above, it has been determined that criminal elements could potentially use this information to gain more knowledge about the department and this would aid them as they attempt to avoid future law enforcement activities.

The release of information under FOI is a release into the public domain and not just to the individual requesting the information. Once information is disclosed by FOI, there is no control or limits as to how the information is shared with other individuals, therefore a release under FOI is considered a release to the world in general.

The Police Service is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. Whilst there is a public interest in the transparency of policing and providing assurance that the Police Service is appropriately and effectively engaging with the threat of criminals/terrorists there is also a very strong public interest in safeguarding the law enforcement role of police.

In addition, PSNI neither confirms nor denies that it holds any other information relevant to the request by virtue of the following exemptions:

Section 23(5) – Information supplied by, or concerning, certain security bodies – confirmation or denial would likely prejudice information directly or indirectly supplied by, or relates to, any specified bodies.

Section 24(2) – National Security – confirmation or denial would likely prejudice safeguarding national security.

Section 31(3) – Law Enforcement – confirmation or denial would likely prejudice the prevention or detection of crime and the apprehension or prosecution of offenders.

'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

Exemptions explained

Section 23 is a class based absolute exemption and there is no requirement to consider the public interest. Confirming or denying the existence of whether any other information is held would contravene the constrictions laid out within Section 23 of the Freedom of Information Act 2000 in that this stipulates a generic bar on disclosure of any information applied by, or concerning, certain Security Bodies.

Section 24 is a qualified exemption and there is a requirement to complete a Public Interest Test in confirmation or denial.

Sections 31 is a prejudice based qualified exemption and there is a requirement to evidence the prejudice (harm) in disclosure and consider the public interest to ensure neither confirming or denying that information is held is appropriate.

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 23(5) – Information supplied by, or relating to, bodies dealing with security matters

Section 1(1) (a) of the Act requires a public authority to confirm whether it holds the information that has been requested. Section 23(5) provides an exemption from this duty. Section 23(5) of the FOIA states that "the duty to confirm or deny does not arise if, or to the extent that, compliance with section 1(1) (a) would involve the disclosure of any information (whether or not already recorded) which was directly or indirectly supplied by, or relates to, any of the bodies specified in subsection (3)."

The police service in its' fight against crime and terrorism may engage at times with the bodies listed at Section 23 of the FOIA and on occasions there may be information provided to police from one of these bodies. As advised above the decision to issue a NCND 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 NCND response is used to avoid risks caused by providing inconsistent responses to a series of similar requests where the information may originate from a number of sources and not necessarily a security body.

Harm in Confirming or Denying that Any Other Information is Held

Any release under FOIA is a disclosure to the world, not just to the individual making the request. To confirm or not whether any other information is or isn't held relating to secondments/ assignments to Regional Organised Crime Units would reveal whether or not PSNI has specific specialist resources within an individual department.

Police forces work in conjunction with other agencies and information is freely shared in line with information sharing protocols. Modern-day policing is intelligence led and this is particularly pertinent with regard to both law enforcement and national security. The public expect police forces to use all powers and tactics available to them to prevent and detect crime or disorder and maintain public

safety. In this case, revealing whether or not a specific ROCU has officers/staff assigned/seconded either to the force or from the force to ROCU, would place PSNI in a vulnerable position by highlighting ROCU activity at force level and within cybercrime units.

The prevention and detection of crime is the foundation upon which policing is built and the threat from terrorism cannot be ignored. It is generally recognised that the international security landscape is increasingly complex and unpredictable. The current UK threat level from internationally terrorism, based on intelligence, is assessed as substantial which means that a terrorist attack is likely.

In order to counter criminal and terrorist behaviour, it is vital that the police have the ability to work together, where necessary covertly, to obtain intelligence within current legislative frameworks to assist in the investigative process to ensure the successful arrest and prosecution of offenders who commit or plan to commit acts of terrorism.

To achieve this goal, it is vitally important that information sharing takes place between police officers, members of the public, police forces as well as other law enforcement bodies within the United Kingdom. Such an action would support counter-terrorism measures in the fight to deprive terrorist networks of this ability to commit crime.

The impact of providing information under FOI which aids in identifying whether or not PSNI has specific roles and resources within their cybercrime unit which are linked to ROCUs would provide those intent on committing criminal or terrorist acts with valuable information.

Public Interest

Section 24(2) National Security

Section 24 - Factors Favouring Confirmation or Denial
The public are entitled to know how public funds are spent and resources distributed within an area of policing, particularly with regard to how the police place resources into their cybercrime units which could lead to terrorist offending. To confirm whether or not any other information exists would enable the general public to hold PSNI to account in relation to tactical resources deployed to police cybercrime offending.

Furthermore, confirming or denying any other information is held may improve public debate and assist the community to take steps to protect themselves.

Section 24 - Factors Against Confirmation or Denial
Taking into account the current security climate within the United Kingdom, no information which may aid a terrorist should be disclosed. To what extent this information may aid a terrorist is unknown, but it is clear that confirmation or denial will have an impact on a force's ability to tactically place secondments from other agencies should they wish to do so.

The public entrust the Police Service to make appropriate decisions with regard to their safety and protection. The only way of reducing risk is to be cautious with what is placed into the public domain.

The cumulative effect of terrorists gathering information from various sources would build a picture of vulnerabilities within certain scenarios, as in this case undermining tactical resources within individual force's cybercrime units.

Section 31(3) Law Enforcement

Section 31 - Factors Favouring Confirmation or Denial
Police forces proactively publish information on their websites relating to their cybercrime units, an example can be found here and this in itself favours confirming information is held.

Section 31 - Factors Against Confirmation or Denial

PSNI has a duty of care to the community at large and public safety is of paramount importance. If an FOI disclosure revealed information to the world (by citing an exemption or stating no information held) that would assist an offender, this would undermine the security of the national infrastructure. Irrespective of what other information may or may not be held, confirmation or denial would reveal tactical capability and vulnerabilities enabling individuals to geographically map which forces have more specialist ROCU resources for cybercrime than others.

By its very nature, confirming or denying whether any other information is held would undermine the effective delivery of operational law enforcement.

Decision

The points above highlight the merits of confirming, or denying, whether any other information pertinent to this request exists. The security of the country is of paramount importance and the Police Service is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. As part of that policing purpose, various operations with other law enforcement bodies may or may not be ongoing. The Police Service will never divulge whether or not any other information is held if to do so would place the safety of individual(s) at risk or undermine National Security.

Whilst there is a public interest in appropriately and effectively engaging with the threat from criminals, there is a very strong public interest in safeguarding National Security. As much as there is a public interest in knowing that policing activity is appropriate and balanced in matters of National Security, this will only be overridden in exceptional circumstances.

The public entrust the Police Service to make appropriate decisions with regard to their safety and protection and the only way of reducing risk is to be cautious with any information that is released. Confirming or denying whether any other information is or isn't held would definitely reveal specialist tactical resource information relating to where ROCUs deploy staff members within cybercrime units and vice versa. This would assist those intent on causing harm. Any incident that results from confirmation or denial would, by default, affect National Security.

Therefore, at this moment in time, it is our opinion that for these issues the balance test for confirming, nor denying, whether any other information is held is made out.

However, this should not be taken as conclusive evidence that any other information exists or does not exist.

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.