CIVIL NUCLEAR CONSTABULARY

The Executive Office
Civil Nuclear Constabulary
Building F6 Culham Science Centre
Abingdon
Oxon
OX14 3DB
Tel: 03303 135400
Website: https://www.gov.uk/cnc

Email

[redacted]

25th June 2021

Dear [redacted]

I am writing in response to your request for information regarding the below**.** Your request has been handled under Section 1(1) of the Freedom of Information Act 2000. In accordance with Section 1(1) (a) of the Act I hereby confirm that the CNC/CNPA does hold information of the type specified.

We are exploring the use of hybrid cloud within public sector organisations in line with the Government Digital Service's (GDS) guidance on 'public sector use of the Public Cloud'. We would like to ascertain whether the cloud-first policy was fit for purpose and what challenges, if any, have arisen when outlining and implementing your cloud strategy.

Please could you provide me with responses to the following questions via electronic copies. If the request is unclear, I would be grateful if you could contact me. If any of this information is already in the public domain, please can you direct me to it, with page references and URLs if necessary.

Please could you confirm you have received this request and I look forward to receiving your responses within the required 20 days of receipt.

FOI questions below and attached.

1. Do you have a cloud strategy? (Please provide a link to the strategy)

- **A) Yes**
- **B) No**

2. When was the cloud strategy defined?

3. If yes, what is the focus of your cloud strategy?

- **A) All in on public cloud (no private cloud or on-premise infrastructure)**
- **B) Cloud First (new services in public cloud with some on premises infrastructure or private cloud)**
- **C) Hybrid cloud (some combination of one or more public clouds, private cloud and on-premises)**
- **D) Private cloud (no public cloud)**

4. What public cloud(s) do you use?

- **A) AWS**
- **B) Alibaba Cloud**
- **C) Azure**
- **D) Google Cloud Platform**
- **E) Oracle Cloud**
- **F) UK Cloud**

5. What percentage of your applications and/or workloads is on premise?

- **A) 0%**
- **B) 10% - 25%**
- **C) 25% - 50%**
- **D) 50% - 75%**
- **E) 100%**

6. What percentage of your applications and/or workloads is in the public cloud?

- **A) 0%**
- **B) 10% - 25%**
- **C) 25% - 50%**
- **D) 50% - 75%**
- **E) 100%**

7. What percentage of your data is on premise?

- **A) 0%**
- **B) 10% - 25%**

C) 25% - 50%
D) 50% - 75%
E) 100%

8. What percentage of your data is in the public cloud?
A) 0%
B) 10% - 25%
C) 25% - 50%
D) 50% - 75%
E) 100%

9. What percentage of your infrastructure is legacy?
A) 0%
B) 10% - 25%
C) 25% - 50%
D) 50% - 75%
E) 100%

10. Do you have third-party services or solutions on premise that are not cloud-ready or fit for cloud migration?
A) Yes
B) No

11. What workloads or functions have you moved to the cloud? (Multiple answers. Please specify other if not listed)
A) Office productivity (e.g. Microsoft 365, Google Workspace)
B) Citizen-facing digital services (e.g. GOV.UK)
C) Back-office applications (e.g. transaction processing)
D) Artificial Intelligence, Machine Learning, cognitive services
E) Software development/DevOps
F) Corporate functions (e.g. HR, Finance, CRM)
G) Intranet
H) Public website
I) Backup, business continuity and disaster recovery
J) Other

12. What challenges did you face when moving to the public cloud? (Multiple answers. Please specify other if not listed)
A) Migrating certain applications
B) Legacy infrastructure
C) Different refresh cycles
D) Difficulty proving cost illustrations
E) Funding paths (Capex/Opex)

F) Data gravity
G) Data Classification
H) Licensing concerns
I) Data privacy concerns
J) Offshoring & data residency
K) Lack of in-house skills
L) Vendor lock-in/ Egress cost prohibitive
M) Other

13. What percentage of your infrastructure do you plan to be public cloud based in 12 months' time?

A) 0%
B) 10% - 25%
C) 25% - 50%
D) 50% - 75%
E) 100%

14. What percentage of your infrastructure do you plan to be public cloud based in three years' time?

A) 0%
B) 10% - 25%
C) 25% - 50%
D) 50% - 75%
E) 100%

15. How much has your organisation spent on public cloud since the Government's G-Cloud or 'cloud-first' policy was introduced in 2012?

16. How much has your organisation spent on on-premise infrastructure since the Government's G-Cloud or 'cloud-first' policy was introduced in 2012?

17. How much has your organisation spent on cloud/infrastructure consultancy services in FY 20-21?

18. How much was spent on public cloud data egress charges in FY 20-21?

1. B
2. Government policy 2013
3. C
4. C

5. A
6. D
7. B
8. D
9. B
10. A
11. A, C, F, G, H, I. A partial NCND is required by virtue of s24(2) National Security, and s31(3) Law Enforcement
12. A, B, G, I, J
13. J
14. E
15. Due to change in systems we are unable to give you the information back to 2021, we can only provide data for the last 18months which is £177,695.76. This cost does not include managing the system as this is considered BAU and therefore is included in our monthly charge.
16. This information will be sent as soon as we have it.
17. £0
18. We are unsure what this is.

For part of question 11 a partial nor confirm nor deny is required by virtue of s24(2) National Security, and s31(3) Law Enforcement. Harm in confirming information is held - Modern day policing is intelligence led and law enforcement depends upon the development of intelligence and the gathering and security of evidence in order to disrupt criminal behaviour and bring offenders to justice. As criminals adapt and exploit new technology, the police need to respond by overcoming hi-tech barriers in order to meet their responsibilities. By revealing whether any other information is held in relation to cloud based data and applications that are extraction technology, will in itself be revealing tactical information which would undermine the process of preventing or detecting crime and the apprehension of prosecution of offenders.

Factors favouring confirming or denial – s31
Confirming or denying that the Civil Nuclear Constabulary force holds further information would raise the general public's awareness around the full extent of policing capabilities and show responsibility to delivery of effective operational law enforcement.

Factors against confirming or denying – s31
By confirming or denying whether further information is held could compromise the Civil Nuclear Constabulary forces law enforcement capabilities and the effectiveness of the force will be reduced. To confirm or deny if further information is held could undermine current and/or future

strategies when carrying out investigations and gathering evidence may be compromised.

The personal safety of individuals is of paramount importance to the Police Service and must be considered in response of every release. A disclosure under Freedom of Information is a release to the world and, in this case, confirming or denying if any further information is held would undermine the evidence gathering process of any investigative inquiry relating to offences, some of which may be serious cases.

Factors favouring confirming or denial – s24
Confirming or denying that any other information exists relevant to the request would lead to a better informed public and the public are entitled to know how public funds are spent. The information simply relates to national security and disclosure would not actually harm it.

Factors against confirming or denial - S24
To confirm or deny whether the Civil Nuclear Constabulary force hold any other information would allow inferences to be made about the nature and extent of national security related activities which may or may not take place. This could enable terrorist groups to take steps to avoid detection, and as such, confirmation or denial would be damaging to national security.

By confirming or denying any policing arrangements of this nature would render national security measures less effective. This would lead to the compromise of ongoing or future operations to protect the security or infra-structure on the UK and increase the risk of harm to the public.

Balancing Test
As always the Freedom of Information Act has a presumption of disclosure, unless when balancing the competing public interest factors the prejudice to the community outweighs the benefits. In this case, there is an argument for confirming or denying, inasmuch as the public have a right to know how forces deliver effective operational law enforcement, and that every effort is made to gather all relevant evidence, including where cloud based data and applications that are extraction technology are used. But this must be balanced against the negative impact these disclosures can make.

Law Enforcement is reliant on community engagement, intelligence and evidence gathering and when it is appropriate, information is given to the public. What has been established in this case is the fact that confirming or denying that any further information relating to technologies is used would

be harmful and have an adverse effect on the investigative process and on the public prevention or detection of crime and the apprehension or prosecution of offenders. This places the victims of such offending at a greater risk towards their health and wellbeing and is not an action the Police Service would be willing to take. These negatives outweigh any tangible community benefit and therefore the balance does not favour disclosure at this time.

The Civil Nuclear Constabulary is a specialist armed police service dedicated to the civil nuclear industry, with Operational Policing Units based at 10 civil nuclear sites in England and Scotland and over 1400 police officers and staff. The Constabulary headquarters is at Culham in Oxfordshire. The civil nuclear industry forms part of the UK's critical national infrastructure and the role of the Constabulary contribute to the overall framework of national security.

The purpose of the Constabulary is to protect licensed civil nuclear sites and to safeguard nuclear material in transit. The Constabulary works in partnership with the appropriate Home Office Police Force or Police Scotland at each site. Policing services required at each site are greed with nuclear operators in accordance with the Nuclear Industries Security Regulations 2003 and ratified by the UK regulator, the Office for Nuclear Regulation (ONR). Armed policing services are required at most civil nuclear sites in the United Kingdom. The majority of officers in the Constabulary are Authorised Firearms Officers.

The Constabulary is recognised by the National Police Chiefs' Council (NPCC) and the Association of Chief Police Officers in Scotland (ACPOS). Through the National Coordinated Policing Protocol, the Constabulary has established memorandums of understanding with the local police forces at all 10 Operational Policing Units. Mutual support and assistance enable the Constabulary to maintain focus on its core role.

We take our responsibilities under the Freedom of Information Act seriously but, if you feel your request has not been properly handled or you are otherwise dissatisfied with the outcome of your request, you have the right to complain. We will investigate the matter and endeavour to reply within 3 – 6 weeks. You should write in the first instance to:

Kristina Keefe
Disclosures Officer
CNC
Culham Science Centre

Abingdon
Oxfordshire
OX14 3DB

E-mail: FOI@cnc.pnn.police.uk

If you are still dissatisfied following our internal review, you have the right, under section 50 of the Act, to complain directly to the Information Commissioner. Before considering your complaint, the Information Commissioner would normally expect you to have exhausted the complaints procedures provided by the CNPA.

The Information Commissioner can be contacted at:

FOI Compliance Team (complaints)
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

If you require any further assistance in connection with this request please contact us at our address below:

Kristina Keefe
Disclosures Officer
CNC
Culham Science Centre
Abingdon
Oxfordshire
OX14 3DB
E-mail: FOI@cnc.pnn.police.uk

Yours sincerely
Kristina Keefe
Disclosures Officer