



19 March 2021

Dear [REDACTED]

**Freedom of Information request: FOI2021/00040**

Thank you for your Freedom of Information request received on the 29 January in which you requested the following:

**Your request:**

*Could you please send me the following regarding your organisation's contracts for the following five areas:*

Category	Service	Key suppliers (incl. connections)	Current Contract Value £k (PA)	Contract: Start Date / End Date		The person responsible for this contract and their contact details
1. Unified Communications:	UC / Telephony					
	Inbound / Outbound Calling					
	Contact Centre					
	Teams Direct Routing					
2. Connectivity:	WAN					
	SD WAN					
	Direct Internet Access					
3. Mobility:	Mobile CTNs					
	Mobile Applications					
	Internet of Things (IoT)					
4. Cloud	Hosted Cloud Services					
5. Cyber Security	Network security					
	Identity and access management					
	Service Operation Centre and Security Incident Event Monitoring					

**Our response**

I can confirm UK Research and Innovation (UKRI) hold some information relevant to your request. Please see the information attached at Annex 1 FOI2021/00040.

Releasing the Network Security and Network security Service Operation Centre and Security Incident Event Monitoring information requested in question 5, would prejudice the prevention or detection of crime as per Section 31(1)(a) of the Freedom of Information Act.

Section 31(1)(a) is a qualified exemption and therefore subject to a public interest test. UKRI applied the Public Interest Test to this request as set out below;

**Public interest in favour of disclosure:**

- There is a public interest in favour of release of the information, to uphold the principles of transparency and accountability, in disclosing information about government or public authority infrastructure and contracts

**Public interest test in favour of withholding the information:**

- The release of this information would make UKRI more vulnerable to crime
- The crime in question would be a malicious attack on UKRI's computer infrastructure and/or systems.
- The release of this information would be seen to prejudice the prevention or detection of crime, by making UKRI's computer systems more vulnerable to hacking and therefore facilitate the possibility of a criminal offence being carried out
- There is an overwhelming public interest in keeping government or public authority computer systems secure, which would be served by non-disclosure.

UKRI has therefore reached the conclusion that, on balance, the public interest is better served by withholding the selected information under Section 31(1)(a).

If you have any queries regarding our response or you are unhappy with the outcome of your request and wish to seek an internal review of the decision, please contact:

Head of Information Governance


Email: [foi@ukri.org](mailto:foi@ukri.org) or [infogovernance@ukri.org](mailto:infogovernance@ukri.org)

Please quote the reference number above in any future communications.

If you are still not content with the outcome of the internal review, you may apply to refer the matter to the Information Commissioner for a decision. Generally, the ICO cannot make a decision unless you have exhausted the review procedure provided by UKRI. The Information Commissioner can be contacted at: <http://www.ico.gov.uk/>

If you wish to raise a complaint regarding the service you have received or the conduct of any UKRI staff in relation to your request, please see UKRI's complaints policy: <https://www.ukri.org/about-us/policies-and-standards/complaints-policy/>

Yours sincerely,

  
Information Governance  
Information Rights Team  
UK Research and Innovation  
[foi@ukri.org](mailto:foi@ukri.org) | [dataprotection@ukri.org](mailto:dataprotection@ukri.org)