Ministry of Defence
D3, Building 405
Corsham
Wiltshire SN13 9NR
United Kingdom

Ref. FOI2015/11086

E-mail: ISS-SecretariatGpMbx@mod.uk

[redacted]

[redacted]

28 January 2016

Dear [redacted]

FREEDOM OF INFORMATION REQUEST

Thank you for your email of 4 December 2015 requesting the following information:

> *"Please provide me any information to current use (areas deployed and topography) of mobile ad-hoc networks by the MOD or any branch of the Armed forces.*
>
> *Please also include where possible any correspondence or files pertaining to the concerns of the reliability and security in the use of mobile ad-hoc networks."*

I am treating your correspondence as a request for information under the Freedom of Information Act 2000.

I wrote to you on 16 December advising that I believed the information you requested would be subject to an exemption under section 24 (National Security) and a public interest test would need to be carried out. I can confirm that the information you requested is not subject to the exemption and therefore a public interest test was not required.

A search for the information you requested has now been completed within the Ministry of Defence (MOD) and I can confirm that some of the information you requested is held.

For the purposes of this response the term "mobile ad-hoc network" is taken to refer to a self-forming network without a dedicated backbone infrastructure or planned laydown. The only MOD deployed tactical mobile communication system that falls within this definition is the High-Capacity Data Radio (HCDR). This is a core capability that provides the main mobile communications backbone at deployed Brigade level and below. It is a tri-service capability, with the Army as the primary user. The radio was brought into service in 2004 and approximately 3,100 HCDR radios are in use by UK Armed Forces. HCDR has been used on the majority of Army deployments of a battle group or more since being brought into service and will continue to be used wherever the UK deploys – so could be used anywhere in the world.

As an ad hoc system, HCDR does not rely upon a fixed topography. The network is self-forming with two levels of hierarchy: a cluster head and cluster members. Cluster heads are automatically nominated from within the radios that will form the network, act as the centre point for nearby HCDR nodes and provide connections between clusters. In the event of loss of a link cluster heads, the system will automatically re-form using the remaining links, including the nomination of a new cluster head if necessary. Design details of the HCDR system are proprietary to Harris Communications.

HCDR uses Class 1 Cryptography, providing a higher level of security than the commercially available export version. HCDR forms a closed network, connecting to wider defence networks via secure gateways. Operational reliability is monitored via standard MOD logistic support processes and no unexpected failure rates have been observed. Drawing on our records of equipment failure rates, the Mean Time Between Activity (MBTA) (The mean time before the radio requires some kind of management or repair attention) for HCDR is 5846 hours and the Mean Time Between Failures (MBTF) is 13627 hours.

No security concerns have been raised on the HCDR network. As such, there are no additional files or correspondence in relation to either of these topics.

With reference to geographical locations, a network of this sort could be deployed by any Army unit on low level training.

Further details of the HCDR radio system are available on the manufacturer's website at the following location:
www.exelisinc.com/solutions/High-Capacity-Data-Radio/Pages/default.aspx

If you are not satisfied with this response or you wish to complain about any aspect of the handling of your request, then you should contact me in the first instance. If informal resolution is not possible and you are still dissatisfied then you may apply for an independent internal review by contacting the Information Rights Compliance team, 1st Floor, MOD Main Building, Whitehall, SW1A 2HB (e-mail CIO-FOI-IR@mod.uk). Please note that any request for an internal review must be made within 40 working days of the date on which the attempt to reach informal resolution has come to an end.

If you remain dissatisfied following an internal review, you may take your complaint to the Information Commissioner under the provisions of Section 50 of the Freedom of Information Act. Please note that the Information Commissioner will not investigate your case until the MOD internal review process has been completed. Further details of the role and powers of the Information Commissioner can be found on the Commissioner's website, http://www.ico.org.uk.

Yours sincerely,

Information Systems and Services (ISS) Secretariat