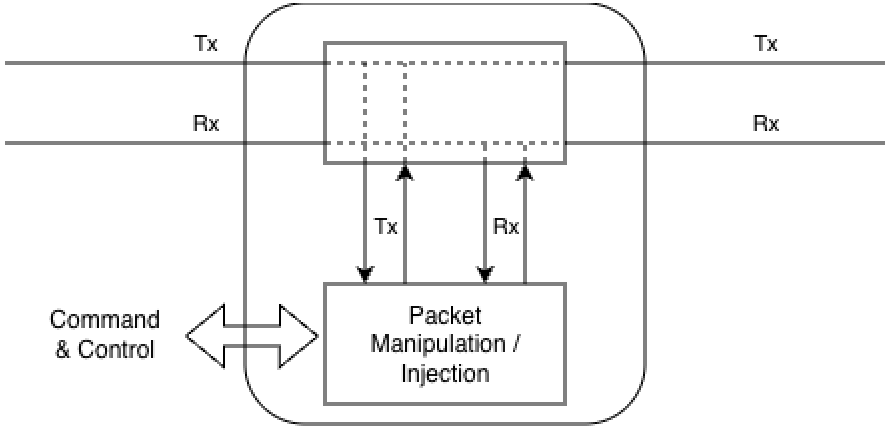
Clarification Q&A in response to the call for proposals

Challenge: **Managing Cyber-Security Risk Through Network Monitoring**

Deadline for questions: 04 November 2025

#	Question	Answer
1.	Is the challenge purely looking for innovations in hardware?	Whilst this challenge has a hardware focus, packet processing is still a requirement for the system as any software we write will need to be able to access them. As such, if you could put together a hardware solution made up of commodity components that has a fail-safe pass-through capability but was not necessarily polished, this would be acceptable so long as it meets the other requirements specified i.e. form factor.
2.	Is the goal to develop a mini network-tap or SOC-like device with observability and packet-injection capabilities?	The objective of the challenge is to have a SOC-like device with observability and packet-injection capabilities and not a mini network-tap.
3.	From a networking perspective, how do you envisage “pass-through” working?	There are any number of ways for this to be implemented. It is up to the team submitting the proposal to have a solution. The main requirement is that a “bypass / pass through” feature is present that allows the device to become electrically or optically transparent in the event of a failure (e.g. loss of power).

4.	Re ‘no passive monitoring’: which active controls are in scope (inline block, RTS/sinkhole, geo-deny)? Any exclusions or ROE guardrails (allowlist, rate-limits, kill-switch)?	This was a constraint to indicate that we are not just interested in passive receipt of packets. The specifics of what active manipulation of traffic takes place will be determined by the project sponsor. We are not looking for assistance with developing the active packet manipulation.
5.	Understand the cost constraints and spec. However, if we want to like for like comparison enterprise products (although more expense) what are the products in the market this solution can be compared with?	There are any number of commercial solutions which offer enterprise level solutions. Gigamon, cPacket and other companies make enterprise grade systems which meet the functional requirements but not the SWaP and cost.
6.	What OSI layers are required and is there a list of protocols which must be mandatory implemented?	Is it envisioned that any solution would allow for access to packets at the IP layer / Layer 3.
7.	Can we get a schematic diagram on how both hardware and software for this project tie to each other?	Below is a very simple schematic. This is deliberately extremely high level so may be of limited use as we do not seek to constrain any solutions being offered.

		 Tx Rx Tx Rx Tx Rx Command & Control Packet Manipulation / Injection
8.	How flexible are you on the critical and essential requirements? If we can demonstrate e.g. cyber capability at higher TRL but hardware (e.g. form factor) at lower TRL will this be dismissed outright or will it still be considered?	The objective for this proposal is the look at alternative hardware platforms. It will depend on what is being proposed but our preference is for higher TRL hardware over software capabilities.
9.	Are there any limitations on location or clearance requirements of developers?	This challenge is open to sole innovators, industry, academic and research organisations of all types and sizes. There is no requirement for security clearances. Solution providers or direct collaboration from countries listed by the UK government under trade sanctions and/or arms embargoes, are not eligible for HMGCC Co-Creation challenges.
10.	Preferred integration/telemetry formats—syslog, NetFlow/IPFIX, STIX/TAXII, REST/Kafka—or vendor-neutral?	No preference at this stage.

11.	For the injection capability is it just matching and replacing content in existing traffic or is it injecting completely new frames?	There is utility in manipulating in flight content and further utility in injecting entirely new content; so both.
12.	How “invisible” is the device expected to be when connected to a network?	It would depend on what layer you were looking for the injection point. It is expected to be visible at the physical layer with an OTDR/TDR etc but invisible when looking at layer 3 and up. Minute changes in latency for specific packets when injecting or manipulating packets are not a concern as long as it doesn’t affect the operation of the receivers of the traffic.
13.	Will sponsors expect or wish to deploy their own software tools or monitoring packages onto the demonstrator during testing?	Not at this stage. We will ultimately look to integrate the system with our own tooling but that will take place later on.
14.	Is the expectation that the total unit cost target of £5,000 applies to both hardware and software, or only to hardware?	The price is intended to be indicative for a piece of hardware that allows us access to monitor and manipulate packets. If there is significant utility in other features that are being proposed then that will be considered separately.
15.	If software licensing or support is required post-project, should indicative annual support costs be included in the overall cost model?	If there are ongoing costs with any solution they should be listed as that will affect the total cost for any solution proposed.
16.	As the challenge references remote access and control, does the sponsor have a preference or requirement to ensure future compatibility with government PQC standards?	There is no requirement for this at this time but if remote access in intrinsic to the proposed solution it should consider how it will align to the NCSC migration timeline for PQC standards.

17.	Is it acceptable for the demonstrator to use an external AC power supply (e.g. laptop-style PSU), or must the design include an integrated mains supply?	There is no requirement for the mains power supply to be integrated. It is accepted that integrating an AC PSU will affect the size and weight of the unit. There is benefit in looking at alternative options for how the unit can be powered.
18.	Should the preferred IP66 rating apply to the in-use configuration, or primarily to the unit in transit or storage?	This refers to the in operation state, not just transport or storage. It expected that there is a trade-off between the SWaP requirements and the available level of ingress protection available. This is only a desirable requirement.
19.	Does the sponsor have a preference for field-level maintenance capability (replacement of NICs, memory, or modules) or would depot-level serviceability be sufficient for evaluation?	This would depend on the nature of the unit but given the cost and SWaP envisioned in the event of an issue the entire unit would be replaced. That is more aligned with the questioner's depot level servicing suggestion.
20.	Would the sponsors find value in a containerised execution environment accessible via the secure management interface, allowing them to deploy or test additional tools within a sandbox?	There needs to be a mechanism to apply rules/control, these will need to be run from somewhere; a containerised solution could be one way to achieve this.
21.	Are there any security or accreditation constraints that would limit sponsor-deployed software?	It is not clear on what those limits would be. The system will need to operate in an environment where it is possible to assure the security of any software deployed by the sponsor e.g. not requiring an internet connection to operate.