Document Details: Q&A in response to the call for proposals

Challenge: Personal Electronics Detector

Deadline for questions: Tuesday 27 May 2025

Questions publish date: Tuesday 3 June 2025

Technical Questions

Q: Is there a maximum necessary range/maximum room size to cover?
A: There is not a maximum range as rooms may vary in size, but it should cover a standard office room (5m x 5m or 20-25sqm).

Q: Is it sufficient to detect only within public cellular band frequencies and public wifi and bluetooth channels?
A: Yes, this is sufficient as most of the devices being targeted are on these public bands.

Q: What is the reason for the requirement to go up to 8GHz? Is this to anticipate future public band usage, or is there already something you currently want to scan for in the 6GHz - 8GHz range?
A: The 8GHz requirement is to cover the future expansion of Wi-Fi 7 channel frequencies, as Wi-Fi 6 is already present. This provides futureproofing of the platform for a period of 3-5 years.

Q: Is it allowable for the detector transmit on WiFi channels, purely for detection purposes?
A: No, the platform is focussed strictly on passive detection; there should be no capability of transmitting

Q: Is there any need to detect WiFi access points and WiFi clients? Or is only detecting WiFi clients sufficient?
A: No, we are only interested in RF energy, there should be no protocol detection.

Q: Will the detector usually be running 24 hours a day, 7 days a week?
A: Yes. Ideally, the platform will be running 24 hours a day, 7 days a week.

Q: Will the detectors always be hard installed or do they need to be moved and used ad hoc sometimes? (The latter could present configuration/set up challenges)
A: There is a possibility for the detectors to be moved when necessary, so the flexibility for this would be ideal. The detectors can be mains powered with a battery back-up; the platform should cater for both hard install and portable operation

Q: In instances where the detectors are hard installed, is it allowable to introduce physical shielding in the room if necessary? I.e. RF attenuative film or paneling.
A: It may be the case that the detector is installed in an area with sufficient shielding already in place, but this would be out of scope for the challenge.

Q: What is the necessary run time for the back up battery?
A: A minimum runtime of 30 minutes, to allow the detector to better handle potential brownouts, power cuts, portable operation, or moving of the unit.

Q: Is it feasible from a security procedure standpoint to use a USB drive to export log information or perform updates?
A: USB functionality may be selected as a suitable method for updates; however, any USB ports must be sealed/made typically inaccessible for unauthorised personnel, such as behind a flap with a security bit screw covering it.

Q: Will the detectors be used in areas that may have high footfall on the outside of the room, or next to rooms where PEDs are allowed? The challenge will be to detect all PEDs inside a room but nothing on the other side of the walls or anyone passing by the outside of the door.
A: This would likely go against provided guidance; however, it is possible that the detector may be positioned near phone lockers in bottleneck areas. The second statement is correct; the platform is for detection of PEDs inside a room, not outside, as a result the detector would need adjustable sensitivity settings.

Q: Are visible external antennas attached to the outside of the enclosure allowed?
A: Yes, external antennas are allowed. The detector is not meant to be overly sensitive as it is meant to work in smaller locations; external antennas may provide higher sensitivity and increase false positive rates.

Q: Is it allowable to use ESP32 microcontrollers (made in China) in the final product?
A: Yes, as long as the supply chain is assured.

Q: Can a configuration setup tool be included. This would be a test transmitter, used during installation of the detector and perhaps an annual calibration, which will aid in setting the correct detector's sensitivity.
A: Yes.

Q: Range – You mention that the Detector will be based in a meeting room. What type of Range are you expecting for the detector? Should this Range or Sensitivity be

manageable by the User/Administrator or would you prefer a pre-defined standard Range?
A: The detector should cover a standard 5mx5m (or 20-25 sqm) office space, although this may be variable and so the range and sensitivity should be able to be adjusted by an administrator.

Q: Alerting – You mention that the detectors "must not inadvertently record sensitive information itself". Would you wish for the detector to store information on *What* type of alert occurred and *When* (with no identifying or sensitive details captured) for later review by a potential central security team (e.g. to analyse trends and find areas where there may be a need for further security awareness training or improvement) or is this seen as an unnecessary requirement?
A: Recorded sensitive information would include the capture of IQ data, which is prohibited under law. The detector should alert with the frequency of a signal, the band, signal strength, and provider if applicable.

Q: Alerting – The Detector should include notifications for the occupants of the room and ideally display the frequency/signal strength/band/provider that caused an alert. Should this display be built into the Detector itself or would it be more appealing to have the ability to show this on a separate display screen linked (securely) to the detector – i.e. is it desirable to have a separate User Interface/Display away from the actual detector device – or would the preference to have a built in display?
A: The display should be built-in as the detector should be a single unit which can be moved or operated portably if necessary.

Q: Alerting – As part of the desirable criteria you mention that you require a passive attribution to a cellular provider. Would it be acceptable to have a "most likely" provider based on passive collect, rather than definite attribution? E.g. Device Detected – Mobile Phone – Probable Vodafone. The assumption is this is to steer meeting room occupants to alert them to the device, rather than to identify the precise device.
A: Yes, this would be acceptable based upon licensed bands. We do not want to pin down a particular device, only draw attention to the presence of a device in the room.

Q: Battery Life – You mention there should be a battery backup. What is the expected life span of the battery backup for the Detector?
A: The battery back-up should last a minimum of 30 minutes to allow the system to deal with power cuts, brown outs, moving of the detector or portable use.

Q: What does "relatively low cost" mean? Less than £100? A few £100?
A: The ideal cost of the detector would be around £2500; however, this is not a target or a limit.

Q: How long should a device be in the space before being detected?
A: A device should be in the space for the shortest possible time which allows for high confidence detection. This is device dependent, for example cellular devices may poll out to a tower anywhere between 2-20 minutes and so should be detected within 20 minutes. For Wi-Fi and Bluetooth, detection should be within a 5-minute period.

Q: Is there a reason 8GHz is chosen as a cut off? UWB signals may go over 8GHz worldwide and those devices are allowed in the UK licence free. Should UWB signals be a target?
A: The 8GHz cutoff was to allow for detection of Wi-Fi 7 and 8. This is a future-proofing requirement to allow the system to remain usable in the future RF space. UWB signals were not considered as a detection source, although this would a welcome addition.