

December 12, 2024

Confidentiality request relating to:

FCC ID: 2BKW7-KERBEROSV21S and IC: 33089-KERBV21S HVIN: V21S

Dear Sir / Madam,

The above-referenced applications request certification of a ground penetrating radar (GPR) device in the USA and Canada, respectively. These applications show that the device complies with each countries' requirements without needing a waiver.

Pursuant to Sections §0.459 and §0.457(d) of the Commission's Rules and §552(b)(4) of Freedom of Information Act, Coded Radar Technologies Pty. Ltd. ("Coded Radar" or the "Applicant") requests, that the Commission grant long-term confidentiality and withhold public disclosure of the following Technical Documents submitted with the above-referenced application:

- a. Schematics
- b. Clock System and Operational Description
- c. Internal Photos
- d. System block diagram

The Applicant similarly requests that Innovation, Science and Economic Development Canada (ISED) grant long-term confidentiality of these submitted Technical Documents.

The above-referenced sections of the Commission's rules authorize it to withhold materials that would be legally privileged if retained by the person submitting them and which would not customarily be released by that person to the public. The listed Technical Documents reveal highly sensitive trade secrets and confidential information belonging to Coded Radar that is not customarily released to the public and which is otherwise unavailable to the public.

The Commission has previously granted long-term confidentially of similar materials submitted with applications for various other GPR devices, including those for FCC ID numbers: QF7NX25, QF7NZ15, QF7FLEXNX, 2ANPE-GP8100, 2ANPE-GS8000, 2ANPE-GP8800, 2ALZQ-PLT600 & 2ALZQ-CO730.

Coded Radar respectfully requests that the Commission grant long-term confidentiality for the listed Technical Documents in relation to FCC certification application ID 2BKW7-KERBEROSV21S.

Coded Radar respectfully requests that ISED grant long-term confidentiality for the listed Technical Documents in relation to application number 33089-KERBV21S HVIN: V21S.

Basis and rationale for the request

Measures taken to prevent unauthorized disclosure

It is understood that the Commission ordinarily denies requests to keep internal photographs confidential where this information could be obtained by a competitor by simply purchasing a device and removing its cover.



The device for which authorization is requested, however, is not a mass-manufactured product that a competitor could easily obtain, disassemble, and study at low cost to them. Rather, it is a relatively expensive device produced in limited quantities that incorporates measures that prevent or dissuade unauthorised disassembly and inspection of internal components.

The existing GPR marketplace is a small and niche field of equipment developers. Within it, only 4 or 5 companies make "3D GPR" systems for the US market. The device for which authorization is requested is within this category. Given the limited scale and resources of the marketplace participants, most guard their trade secrets and technical knowhow embodied within their GPR products by making them difficult to disassemble and by keeping precise details of internal components, system configuration and the exact approach confidential.

Coded Radar has taken similar steps to ensure the internal circuitry and workings of the device for which authorization is sought remains inaccessible to unauthorized persons. Particular attention has been applied to the NM-GPR V2.1 digitizer, the main system component (see Internal Photos A). To protect the confidentiality of its internal details, the machined metal enclosure has been secured using custom-designed security screws that are also adhered in place. These can only be removed using a unique tool only available to Coded Radar. Without the tool, access to the internal circuits would require destructive cutting or grinding through the enclosure, which is likely to permanently damage internal components. Operators of the device are also dissuaded from equipment disassembly or tampering via warnings and security stickers. As stated in the User's Manual *"Tampering, modification or unauthorized access to the internal components of this equipment, as determined in the opinion of Coded Radar and at their sole discretion, will render the warranty null and void."* Custom-made tamper-evident security stickers have also been placed at key locations on the case exterior, ensuring any attempts to open it would be detected. Coded Radar would refuse to repair any device showing signs of unauthorized disassembly or tampering.

Competitive harm to the Applicant

The device seeking authorization uses several unique techniques to achieve far greater GPR performance while remaining compliant with the Commission's rules. These capabilities are unique within the field of GPR, and their introduction is likely to provide significant benefits for US customers.

The listed Technical Documents submitted with this application, reveal a variety of sensitive details including how the device operates, manufacturing details, and design information that could be used by competitors to estimate equipment production costs and sales margins. The information contained in these documents has never been made public and previous disclosure of this information to third parties has been limited to only those directly involved in device development or jurisdictional authorization.

Disclosure of the commercially sensitive details within these documents would cause substantial competitive harm to the Applicant, by revealing confidential information about internal workings of the device and its design features created at significant expense and effort by the Applicant. Disclosure of these documents would also unfairly benefit competitors, by revealing sensitive details of the Applicant's development and engineering work that competitors would not otherwise have access to.



Commercial value of information

Development of the device hardware took the Applicant approximately two years to complete, with firmware development and refinement taking significantly longer. This in turn required considerable research, development and engineering efforts by the Applicant over a long period. Given the development time and cost involved, Coded Radar suggests that it would be appropriate and justified for the Commission to grant long-term confidentiality of the listed Technical Documents.

If undisclosed, key details contained within the listed Technical Documents could only be acquired by competitors by expending similar resources and effort over several years. Alternatively, competitors might attempt to copy the equipment, although this would involve considerable cost and risk.

The device is usually sold as part of the Kerberos[™] platform, which retails for more than USD \$150,000. A competitor wanting to copy the system would, therefore, first need to purchase the equipment, then void its warranty by tampering and finally risk damaging or destroying the internal circuits by cutting or grinding through the metal case. Even if successful in obtaining access to the circuits, the device operation might still not be understood, making this approach expensive, risky, and ultimately unsuccessful.

The information revealed by the listed Technical Documents, therefore, is of considerable commercial value if it remains undisclosed. It is also difficult and expensive to obtain by surreptitious means.

Conclusion

As outlined in the preceding sections, disclosure of the listed Technical Documents, which are not ordinarily available to the public, is likely to cause substantial competitive harm to Coded Radar and would unfairly benefit competitors by revealing important trade secrets and key equipment details developed over many years at great cost and with substantial effort.

Considering the risk of competitive harm to the Applicant, the substantial commercial value of the information revealed by these documents, and significant cost and difficulty for competitors to obtain this information by other means, Coded Radar respectfully requests that the Commission and ISED grant long-term confidentiality of the listed Technical Documents in relation to FCC Certification Application ID 2BKW7-KERBEROSV21S and IC application 33089-KERBV21S HVIN: V21S, respectively.

The Applicant respectfully requests that the listed Technical Documents be returned if the Commission decides to decline granting long term confidentiality, in accordance with §0.459(e) of the Commission's rules.

Sincerely,

Dr Bryan Reeves **Chief Technology Officer** Coded Radar Technologies Pty. Ltd. Unit 1, 75 Bluestone Circuit, Seventeen Mile Rocks, Queensland, AUSTRALIA 4073

Page | 3