

To: Federal Communications Commission
7435 Oakland Mills Road
Columbia, MD 21046
USA

Date: July 12, 2023

Attestation

**Section 2.911(d)(5)(i) and Section 2.911(d)(5)(ii)
(KDB 986446 D01 Covered Equipment)**

Section 2.911(d)(5)(i)

Riedel Communications GmbH & Co. KG ("the applicant") certifies that the equipment for which authorization is sought is not "covered" equipment prohibited from receiving an equipment authorization pursuant to section 2.903 of the FCC rules.

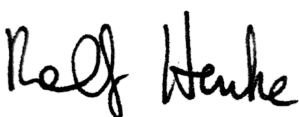
Section 2.911(d)(5)(ii)

Riedel Communications GmbH & Co. KG ("the applicant") certifies that, as of the date of the filing of the application, the applicant **is not** identified on the Covered List (as a specifically named entity or any of its subsidiaries or affiliates) as an entity producing "covered" equipment.

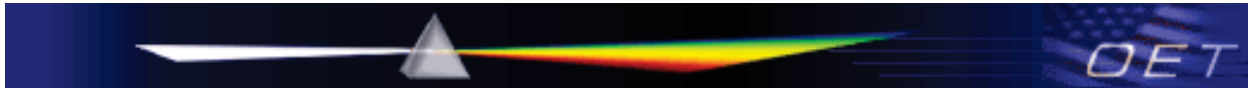
Type of equipment subject to FCC Certification: Intercom Matrix with integrated RFID reader

FCC ID: YFJART1024

Contact Person:	Ralf Henke
Position in the Company:	Head of Hardware Development
Date of Signature:	July 12, 2023



Signatory
(Signature of the applicant)



**Federal Communications Commission
Office of Engineering and Technology
Laboratory Division**

April 10, 2023

**PROTECTING AGAINST NATIONAL SECURITY THREATS TO THE COMMUNICATIONS
SUPPLY CHAIN THROUGH THE EQUIPMENT AUTHORIZATION PROGRAM**

A. INTRODUCTION

On November 25, 2022, the FCC released [FCC 22-84](#), a *Report and Order, Order, and Further Notice of Proposed Rulemaking* on “Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program.”

In the Report and Order portion of FCC 22-84, the Commission adopted new FCC requirements to protect the nation’s networks and supply chains from certain equipment (“covered” equipment) that poses an unacceptable risk to national security or the safety of U.S. persons. Specifically, the Commission adopted rules that prohibit equipment authorization for “covered” telecommunications equipment and video surveillance equipment produced by entities identified on the Commission’s Covered List, which is periodically updated.¹ See the [Covered List](#) for more details.

The rules prohibiting authorization of “covered” equipment, adopted in the Report and Order portion of FCC 22-84, became effective upon publication in the Federal Register on February 6, 2023.

The current Covered List identifies the following telecommunications and video surveillance equipment, produced by certain entities, as “covered” equipment:

- “Telecommunications equipment” and “video surveillance equipment” produced by Huawei Technologies Company (Huawei) or ZTE Corporation (ZTE), or by any subsidiaries or affiliates of such entities;
- “Telecommunications equipment” and “video surveillance equipment” produced by Hytera Communications Corporation (Hytera), Hangzhou Hikvision Digital Technology Company (Hikvision), or Dahua Technology Company (Dahua), or by any subsidiaries or affiliates of such entities, “for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purpose.”

Until the date that the new rules became effective, in FCC 22-84 the Commission adopted an interim “freeze” Order (paragraphs 264-66) on equipment authorizations prohibiting TCBs from approving authorization of any equipment produced by Huawei, ZTE, Hytera, Hikvision, or Dahua, or by any of their respective subsidiaries or affiliates.

¹ The Commission’s [Covered List](#) is published by the Public Safety and Homeland Security Bureau and posted on the Commission’s website. This Covered List, which is periodically updated, identifies particular equipment, produced by particular entities, that constitutes “covered” equipment.

B. QUESTIONS AND ANSWERS

1. Do the new rules require new information to be submitted as part of the equipment authorization process? Yes, upon the rules becoming effective, additional information is required with every equipment authorization submission. These include the following:

- a. *Certifications concerning “covered” equipment.* Section 2.911(d)(5)(i)-(ii) of the rules require two certifications by the applicant at the time that the application for equipment authorization is filed with the TCB. These certifications can be submitted together in one submission.
 - i. The applicant for equipment authorization must provide a written and signed certification that the equipment for which it seeks an equipment authorization is not prohibited from receiving an equipment authorization pursuant to section 2.903. Section 2.903 (a) prohibits authorization of “covered” equipment. Accordingly, the applicant must submit a written and signed certification that the equipment for which it seeks authorization is not “covered” equipment.

The applicant should provide the information required by section 2.911(d)(5)(i) as an attachment to their equipment authorization application (the attachment should be uploaded as a PDF document to the exhibit type “Attestation Statements” with the description text identifying it as the section 2.911(d)(5)(i) filing), and do so in a manner similar to the following example:

[Insert applicant name] (“the applicant”) certifies that the equipment for which authorization is sought is not “covered” equipment prohibited from receiving an equipment authorization pursuant to section 2.903 of the FCC rules.

The applicant must sign this certification.

If the equipment for which the applicant seeks authorization is produced by any of the entities identified on the current Covered List, the applicant should include an explanation on why the equipment is not “covered” equipment.

- ii. The applicant for equipment authorization must provide a written and signed certification that includes an affirmative or negative statement as to whether the applicant is identified on the Covered List, established pursuant to section 1.50002, as an entity producing “covered” equipment. Entities identified on the current Covered List as producing “covered” equipment include Huawei, ZTE, Hytera, Hikvision, and Dahua, and their subsidiaries and affiliates. If the applicant is any one of these entities (i.e., an entity specifically named on the Covered List or any of its subsidiaries or affiliates), it must include a written and signed certification in the affirmative; if the applicant is not any one of these entities, it must include a written and signed certification in the negative.

The applicant should provide the information required by section 2.911(d)(5)(ii) as an attachment to their equipment authorization application (the attachment should be uploaded as a PDF document to the exhibit type “Attestation Statements” with the description text identifying it as the section 2.911(d)(5)(ii) filing), and do so in a manner similar to the following example:

[Insert applicant name] (“the applicant”) certifies that, as of the date of the filing of the application, the applicant [is / is not] identified on the Covered List (as a specifically named entity or any of its subsidiaries or affiliates) as an entity producing “covered” equipment .

The applicant must sign this certification.

- b. *Certification designating a U.S. agent for service of process.* As required by section 2.911(d)(7), the applicant must designate a contact located in the United States for purposes of acting as the applicant’s agent for service of process, regardless of whether the applicant is a domestic or foreign entity. An applicant located in the United States may designate itself as the agent for service of process.

In either scenario, the designation of the U.S. agent for service of process should be provided as an attachment to the equipment authorization application (the attachment should be uploaded as a PDF document to the exhibit type “Attestation Statements” with the description text identifying it as the section 2.911(d)(7) filing). The applicant must provide a written certification, which must:

- i. Be signed by both the applicant and designated agent for service of process, if the agent is different from the applicant.
- ii. Acknowledge the applicant’s consent and the designated agent for service of process’s obligation to accept service of process.
- iii. Provide a physical U.S. address and email for the designated agent for service of process.
- iv. Acknowledge the applicant’s acceptance to maintain an agent for service of process for no less than one year after the grantee has terminated all marketing and importation or the conclusion of any Commission-related proceeding involving the equipment.

- 2. How should TCBs address applications for authorization of telecommunications equipment and video surveillance equipment produced by Hytera Communications Corporation (Hytera), Hangzhou Hikvision Digital Technology Company (Hikvision), or Dahua Technology Company (Dahua), or by any subsidiaries or affiliates of such entities?** At this time, TCBs must not grant authorization of any telecommunications or video surveillance equipment produced by any of these entities. Before any such grant will be permitted, further Commission approval is required.

In FCC 22-84 (paragraph 177), the Commission prohibits authorization of telecommunications and video surveillance equipment produced by Hytera, Hikvision, or Dahua, or by any subsidiaries or affiliates of such entities, “[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes.” The FCC will only conditionally approve authorization of this equipment after certain conditions are met. In FCC 22-84 (paragraph 180), the Commission provides that *before* the Commission will permit equipment authorization of such telecommunications and video surveillance equipment, Hytera, Hikvision, and Dahua first must seek and then obtain Commission approval of their respective plans associated with marketing or sale of such equipment that will ensure that this equipment will not be marketed or sold for any of the prohibited purposes. If and when the Commission allows authorization of telecommunications and video surveillance for any of these entities, this guidance will be updated.

3. **Are all applicants required to submit certifications regarding “covered” equipment for all equipment authorization applications?** Yes, the certifications are required for all applications received after the effective date of the rules, regardless of the type of equipment or whether the equipment is produced by an entity identified on the Covered List as producing “covered” equipment.
4. **Can the certifications provided to the FCC for compliance with section 2.911(d)(5) and 2.911(d)(7) requirements be confidential upon submission to the FCC?** No. These certifications are not confidential.
5. **How does the Commission define subsidiaries and affiliates?** The new rules, at section 2.903(c), define affiliates and subsidiaries. The term “affiliate” means an entity that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another entity; for purposes of this paragraph, the term ‘own’ means to have, possess, or otherwise control an equity interest (or the equivalent thereof) of more than 10 percent. The term “subsidiary” means any entity in which another entity directly or indirectly (1) holds de facto control or (2) owns or controls more than 50 percent of the outstanding voting stock.
6. **What is “telecommunications equipment”?** FCC 22-84 (paragraph 195) provides that telecommunications equipment means any equipment used in fixed or mobile networks that provides advanced communications service, provided the equipment includes or uses electronic components. This encompasses any equipment that can be used in such a fixed or mobile broadband network to enable users to originate and receive high quality voice, data, graphics, and video telecommunications using technology with connection speeds of at least 200 kbps in either direction. Additional guidance on telecommunications equipment is set forth in FCC 22-84.
7. **What is “video surveillance equipment”?** FCC 22-84 (paragraph 205) provides that video surveillance equipment includes any equipment that is used in fixed and mobile networks that provides advanced communications service in the form of a video surveillance service, provided the equipment includes or uses electronic components. This encompasses any equipment that can be used in such a fixed or mobile broadband network to enable users to originate and receive high quality voice, data, graphics, and video telecommunications using technology with connection speeds of at least 200 kbps in either direction. Additional guidance on video surveillance equipment is set forth in FCC 22-84.
8. **How should a Telecommunications Certification Body (TCB) proceed if there is a reasonable basis for questioning the certifications concerning “covered” equipment?** Pursuant to TCB responsibilities under section 2.962(f)(1), TCBs are expected to evaluate all applications to ensure compliance with Commission requirements. These requirements now include prohibiting authorization of “covered” equipment, and TCBs are expected to exercise appropriate diligence to prohibit granting of “covered” equipment. Since TCBs are responsible for prohibiting authorization of “covered” equipment, TCBs should not rely solely on the applicant’s certification. If, in evaluating an application for compliance with this prohibition, the TCB has reason to believe that the subject equipment is or may be “covered,” the equipment should not be authorized, the TCB should not process the application.

The TCBs also should notify the FCC of any certification regarding “covered” equipment that the TCB believes may not be accurate with respect to whether the equipment is produced by an entity identified on the Covered List (i.e., an entity specifically named on the Covered List or any of its subsidiaries or affiliates) or whether the equipment is not “covered.” With regard to these issues, TCBs should submit a Knowledge Database (KDB) inquiry to the FCC at www.fcc.gov/KDB including information about the equipment, information about the applicant, a description of how the TCB evaluated the information for compliance and the TCB’s specific question(s). The KDB categories for “covered” equipment questions are – First Category: Covered Equipment, Second Category: Covered Equipment.

- 9. What should a TCB do if it grants an equipment authorization but later concludes that the equipment is “covered” equipment or otherwise should have been prohibited from equipment authorization?** Each TCB should have documented procedures in place to ensure that all requirements are evaluated and found to be compliant before issuing any equipment authorization. In cases where a TCB concludes that an equipment authorization was improperly granted, the TCB should immediately submit a KDB inquiry explaining the issue to the FCC and the FCC will review the information, and if appropriate, set the equipment authorization grant aside and dismiss the application.
- 10. What actions can the FCC take regarding TCBs that grant equipment authorizations for “covered” equipment?** The FCC will review each such occurrence on a case-by-case basis to determine what action is appropriate. Pursuant to TCB responsibilities under section 2.962(f)(1), TCBs are expected to evaluate all applications to ensure compliance with Commission requirements. These requirements include prohibiting authorization of “covered” equipment, and TCBs are expected to exercise appropriate diligence to prohibit granting of “covered” equipment. In the event that a TCB grants an authorization of equipment that is later determined to be “covered” equipment, the FCC will review each such occurrence on a case-by-case basis to consider the circumstances of the grant and to determine whether any action may be called for or appropriate.
- 11. When a TCB completes a Form 731 application will there be a separate scope for “covered” equipment?** No, there will not be a separate scope created for “covered” equipment.
- 12. Can a TCB serve as an applicant’s (grantee’s) agent for service of process?** The Commission (FCC 22-84) requires each applicant (grantee) to designate a U.S. legal entity as its agent for service of process. Although FCC 22-84 does not explicitly prohibit a TCB from serving as an agent for service of process, the ability of a TCB to act as an agent for service of process for an applicant (grantee) may conflict with the requirement that TCBs be impartial in their approval of devices and not provide consultancy to applicants (grantees) (see International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), 17065). The opportunity to gain an additional revenue stream from successful but not from unsuccessful applicants (grantees) could impact a TCB’s ability to remain objective in evaluating applications for equipment authorizations. There is a similar concern about testing labs’ objectivity. Therefore, these entities (including their employees, subsidiaries, and affiliates) should NOT serve as an agent for service of process.
- 13. Must the agent for service of process be located in the United States?** Yes. The agent for service of process (an individual or an entity) must be located in the United States.

- 14. Can the U.S. agent for service of process be located in a U.S. territory or possession?** Yes.
- 15. Must the agent for service of process sign the application?** The agent for service of process does not sign the application itself. However, the applicant (grantee) must provide a written certification designating the agent for service of process, and both the applicant and the agent for service of process must sign this certification designation pursuant to section 2.911(d)(7). The agent for service of process, by signing that certification designation letter, is agreeing to serve as the agent for service of process, and the applicant (grantee), by making that designation, is consenting to service upon the agent for service of process as legally sufficient to constitute service on the applicant (grantee).
- 16. Who can sign the written certifications required by 47 CFR § 2.911(d)(7), including the certifications associated with the applicant's (grantee's) designated agent for service of process?** The applicant (grantee) contact of record in the equipment authorization system or authorized officers or employees of the applicant (grantee) must sign the required certifications, including the one designating the agent for service of process. The agent for service of process also must sign the written certification of designation indicating acknowledgment of their obligation to accept service of process.
- 17. Can an agent for service of process sign certifications on behalf of the applicant (grantee)?** No, unless the designated agent for service of process is a duly authorized officer or employee of the U.S.-based applicant (grantee).
- 18. Is the agent for service of process required to have an FRN?** If the agent for service of process does business with the FCC, it should have an FRN, and that FRN is required to be included on the attachment/certification letter designating the agent for service of process. If the agent for service of process does no business with the FCC other than being designated as an U.S agent for service of process, a separate FRN is not required; in such case, only the grantee's FRN is required to be included on the attachment/certification letter designating the U.S. agent for service of process.
- 19. If the applicant (grantee) is located in the U.S., can it be its own agent for service of process?** Yes. If the applicant (grantee) chooses to be its own agent for service of process, the applicant (grantee) still must submit a certification, including the required contact information for the agent for service of process, designating itself and agreeing to accept service of process.
- 20. Does the applicant's written certification designating its agent for service of process need to be provided in an exhibit that is unique to the specific FCC ID in the application? Can the designation cover all products for a given applicant?** Each application must have a specific, valid written certification designating the agent for service of process. The applicant (grantee) should ensure that the designated agent for service of process is aware of and accepts its obligation as agent for service of process for each application. The agent for service of process is required to sign the certification designation letter accepting such designation/agreeing to act as agent for service of process. An applicant (grantee) can use the same agent for service of process for different applications, but each application specifically must designate an agent for service of process.

- 21. Can the written certification designating the agent for service of process include an expiration date?** No, the written certification designating the agent for service of process is not permitted to have an expiration date.
- 22. What is the minimum required term for an agent for service of process?** The grantee must maintain an agent for service of process at all times that the device is marketed and for at least one year past the termination of marketing of the device. There is no minimum required term for an agent for service of process. The grantee may change the designated agent for service of process at any time in accordance with section 2.929 of the Commission's rules.
- 23. What are the responsibilities of the agent for service of process?** An agent for service of process for the particular equipment certification authorization has the obligation to accept the service of process and other legal process documents on behalf of the grantee of the authorization (the responsible party) and to swiftly and dutifully deliver them to that party. Service of process includes, but is not limited to, delivery of any correspondence, notices, orders, decisions, and requirements of administrative, legal, or judicial process related to Commission proceedings. See FCC 22-84, paragraph 63. However, service of process on the grantee of the equipment authorization is deemed to be complete when the document is sent to the U.S. physical address, U.S. mailing address (if different), or e-mail address of the U.S.-based agent for service of process.
- 24. If there is an investigation or enforcement matter, is the agent for service of process required to cooperate?** Yes, insofar as the agent for service of process is obligated to accept the service of process and other legal process documents on behalf of the grantee of the authorization (the responsible party) and to swiftly and dutifully deliver them to that party.
- 25. What happens, and what are the responsibilities of (a) the grantee and (b) the agent for service of process, when the agent for service of process can no longer act as the grantee's agent for service of process?** It is the responsibility of the grantee to maintain an agent for service of process at all times that the device is marketed and for at least one year past the termination of marketing of the device. See FCC 22-84, paragraph 64. Grantees must promptly, and in any event, within 30 days after changing the agent for service of process, notify the Commission, via the granting TCB, of any change in the agent for service of process. See Section 2.929(c). Keep in mind that service of process on the grantee of the equipment authorization is deemed to be complete when the document is sent to the U.S. physical address, U.S. mailing address (if different), or e-mail address of the U.S.-based agent for service of process on file with the Commission at the time of such service.
- 26. If the agent for service of process for an authorization is either unwilling or unable to fulfill its obligation, are there any consequences on the part of the agent for service of process?** First, the agent for service of process, when signing the designation letter in the application for equipment authorizations, is agreeing to serve as the agent for service of process for the applicant (grantee) and remains obligated to do so unless and until replaced by the grantee. Since service upon the designated agent for service of process is considered legally sufficient notice/service to the applicant (grantee), the consequences of an agent for service of process that fails to fulfill its obligations could be detrimental to the applicant (grantee). Once the agent for service of process is served, the grantee is deemed served and accordingly subject to any applicable consequences resulting from being served.
- 27. Can the grantee refuse to accept service of process from the Commission if the Commission serves process on the grantee's agent for service of process?** No. Accordingly, grantees should carefully choose their agent for service of process because service on the designated agent for service

of process WILL constitute service on the grantee, whether or not the grantee believes the agent for service of process properly informed the grantee.

- 28. Can the agent for service of process designation or the agent for service of process contact information be changed after the grant of equipment authorization?** Yes, so long as necessary procedures are followed. Grantees must promptly, and in any event, within 30 days after changing the agent for service of process, notify the Commission, via the granting TCB, of any change in the agent for service of process. See Section 2.929(c). The TCB should submit a KDB inquiry explaining the change and requesting the FCC to put the application in audit mode. The FCC will notify the TCB once the request has been approved or if additional information is required. It is the responsibility of the grantee to maintain an agent for service of process at all times that the device is marketed and for at least one year past the termination of marketing of the device. See FCC 22-84, paragraph 64.
- 29. Must the test report include all information required by section 2.1033(b) and (c) regarding the U.S agent for service of process—full name, mailing address and physical address (if different), email address, and telephone number of the applicant (grantee) and the applicant’s (grantee’s) agent for service of process in the United States?** The FCC requirements for the content of the test report have not changed as a result of FCC 22-84 and the test reports should continue to clearly identify for whom the testing was performed. The new written certifications concerning the U.S. agent for service of process that are required by FCC 22-84 should be separately submitted to the “attestation statement” exhibit type folder as part of the equipment authorization application.
- 30. Are the written certifications and designation of agent for service of process required for permissive change such as class 2 and class 3 permissive changes and change in FCC IDs?** Yes. The certifications are required for class 2 and class 3 permissive changes and changes in identification of equipment. See 47 CFR §§ 2.1043(b)(2)(i)(D)-(E), 2.1043(b)(3)(i)(D)-(E), 2.933.
- 31. Will the FCC provide advance notice or general notification to TCBs regarding publication of an updated Covered List?** No. The FCC will issue a public notice whenever it updates the Covered List that identifies “covered” equipment. TCBs are responsible for complying with the most recent Covered List.
- 32. If a TCB receives an application for equipment that is produced by an entity identified on the Covered List – either as an entity specifically named on the Covered List or an entity that is a subsidiary or affiliate of such entity – is an explanation of why the equipment is not covered required?** The FCC rules require the submission of a written and signed certification as to whether the equipment is “covered” equipment along with a statement as to whether the applicant is identified on the Covered List (i.e., is any entity specifically named on the Covered List or any of its subsidiaries or affiliates). A TCB, however, cannot simply rely on the signed certification; unless the TCB has sufficient information to determine that the equipment is not covered, it should not authorize the application. Unless it is clear from the application itself that the equipment is not covered, prior to authorizing the device, the TCB must do sufficient due diligence and may be required to provide an explanation of why the equipment is not covered. TCBs may submit a KDB request for OET staff guidance.
- 33. If the TCB receives an application from an entity identified on the Covered List, with a written certification that the equipment is not “covered,” and an explanation of why the equipment is not covered, must the TCB receive any approval from the FCC to authorize the application?** No, FCC approval is not required for the TCB to authorize the application of an entity identified on the Covered List. Note that even if the applicant certifies that the equipment is not “covered,” the

TCB remains responsible for evaluating whether the equipment is or is not “covered,” and ensuring that the TCB does not authorize “covered” equipment. If the TCB has a concern or sees ambiguity in the application about whether the equipment is “covered,” the TCB should submit a KDB request for FCC guidance.

- 34. Can TCBs issue a grant for applications for certification of equipment submitted by entities that produce “covered” equipment if the equipment for which certification is sought is not “covered,” such as audio speakers?** Generally, yes, so long as the application for certification concerns equipment that is not telecommunications or video surveillance equipment and, therefore is not “covered.”
- 35. Can a TCB authorize equipment authorization applications for equipment produced by entities identified on the Covered List if that equipment is not “covered” equipment?** If the TCB determines that the equipment for which authorization is sought is produced by Huawei or ZTE (or by any of their subsidiaries or affiliates) and is not “covered” telecommunications or video surveillance equipment, then the TCB may authorize the equipment so long as all other certification requirements are met. At this time, TCBs cannot authorize any telecommunications or video surveillance equipment produced by Hytera, Hikvision, and Dahua, because of special requirements currently applicable to such equipment.
- 36. Are there special requirements pertaining to authorization of telecommunications or video surveillance equipment produced by Hytera, Hikvision, and Dahua (and their subsidiaries or affiliates)?** Yes. In FCC 22-84 (paragraph 177), under the prohibition on authorization of “covered” equipment, the Commission prohibits authorization of any telecommunications and video surveillance equipment produced by Hytera, Hikvision, or Dahua (or by any subsidiaries or affiliates of such entities) “[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes.” The FCC will only conditionally approve authorization of this equipment if and after certain conditions are met. At this time, those conditions have not been met. Accordingly, at this time the FCC prohibits authorization of any telecommunications or video surveillance equipment produced by Hytera, Hikvision, and/or Dahua.
- In FCC 22-84 (paragraph 180), the Commission provides that *before* the Commission will permit equipment authorization of such telecommunications and video surveillance equipment, Hytera, Hikvision, and Dahua first must first obtain Commission approval of their respective plans associated with marketing or sale of such equipment that will ensure that this equipment will not be marketed or sold for any of the prohibited purposes. If and when the Commission allows authorization of telecommunications and video surveillance for any of these entities, this guidance will be updated.
- 37. Can equipment produced by any of the entities identified on the Covered List be authorized pursuant to the SDoC process if the responsible party that seeks to use the SDoC process believes that such equipment is “not” covered equipment?** No. As of February 6, 2023, no equipment that is produced by any of the entities that produce “covered” equipment (whether an entity named on the Covered List or any of its subsidiaries or affiliates) can obtain equipment authorization through the SDoC authorization option. Equipment authorization of this equipment may be granted only through the certification process.
- 38. Can equipment produced by any of the entities identified on the Covered List be exempted from the need for equipment authorization if the entity seeking exemption believes that such equipment is “not” covered equipment?** No. As of February 6, 2023, no equipment that is produced by any of the entities that produce “covered” equipment (whether an entity specifically

named on the Covered List or any of its subsidiaries or affiliates) can be exempted from the need for an equipment authorization; such equipment can only obtain authorization through the certification process.

- 39. Will the FCC provide resources for TCBs to use to check for affiliations between an applicant and the entities identified on the covered list?** The Commission’s rules define “subsidiaries” and “affiliates” in section 2.903(c). The entities specifically named on the Covered List are required, pursuant to section 2.903(b), to provide to the FCC information on their subsidiaries and affiliates; these filings are now public in the FCC’s [ECFS](#) system, and will be posted on the FCC’s equipment authorization website. The FCC may provide additional information resources. In any event, in exercising their responsibilities, TCBs should not rely solely on these filings or resources, but should consult that information as they evaluate applications for compliance with the Commission’s requirements. TCBs also have the responsibility in their evaluation to exercise appropriate diligence if they have reason to believe that an applicant has failed to disclose that it is a subsidiary or affiliate of an entity named on the covered list. TCBs will be held responsible for any grants issued to entities with affiliations they knew or reasonably should have known.
- 40. Must applicants certify that there are no components within the equipment which could be construed as being “covered” equipment?** The Commission does not currently require that applicants, when certifying that the equipment is not “covered,” address whether any component part of that equipment is “covered” equipment.
- 41. Given the Commission’s prohibition on authorization of “covered” equipment, are written certifications on the issue of “covered” equipment now required for all equipment authorized through the SDoC process?** Yes. Section 2.938(b)(2) requires that the responsible party for *any* equipment authorized through the SDoC process retain, as part of its records, a signed written certification that, as of the date of first importation or marketing of equipment, such equipment is not produced by any entity identified on the Covered List i.e., an entity specifically named on the Covered List or any of its subsidiaries or affiliates) as producing “covered” equipment.
- 42. In the case of a permissive change to authorize use of a certified module in a specific host device, must the host manufacturer provide the attestations required by 2.911(d)(5) and/or (d)(7), or can it simply rely on the previous authorization of the module?** Any new application by a host manufacturer must include the attestations required by 2.911(d).
- 43. What requirements apply when changes are made to “covered” equipment authorized prior to the effective date of FCC 22-84, such as placing a different modem inside a camera system?** When any changes are made to a device, the 2.1043 permissive change rules apply. However, if the change involves “covered” equipment, even if the original equipment was authorized before the effective date of FCC 22-84, the TCB is prohibited from authorizing that equipment. All class 2 and class 3 permissive changes require filings certifying the equipment is not otherwise prohibited from receiving an equipment authorization. In addition, the filing must also designate an agent for service of process, along with the certification required under section 2.911(d)(7).

CHANGE NOTICE

04/10/2023: 986446 D01 Covered Equipment Guidance V02 replaces 986446 D01 Covered Equipment v01: Changes include modifying the template to conform with latest FCC KDB template, minor edits to the introduction section, and adding new guidance items 12 through 43.



PUBLIC NOTICE

Federal Communications Commission
45 L St., N.E.
Washington, D.C. 20554

News Media Information 202 / 418-0500
Internet: <https://www.fcc.gov>
TTY: 1-888-835-5322

DA 22-979

Released: September 20, 2022

PUBLIC SAFETY AND HOMELAND SECURITY BUREAU ANNOUNCES ADDITIONS TO THE LIST OF EQUIPMENT AND SERVICES COVERED BY SECTION 2 OF THE SECURE NETWORKS ACT

WC Docket No. 18-89, ET Docket No. 21-232, EA Docket No. 21-233

Pursuant to sections 2(a) and (d) of the Secure and Trusted Communications Networks Act of 2019 (Secure Networks Act),¹ and sections 1.50002 and 1.50003 of the Commission's rules,² the Federal Communications Commission's Public Safety and Homeland Security Bureau (Bureau) announces the following additions to the list of communications equipment and services (Covered List) that have been determined by Executive Branch interagency bodies to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons.³ The updated Covered List reproduced in the Appendix to this Public Notice is also found on the Bureau's website at <https://www.fcc.gov/supplychain/coveredlist>.

The *Supply Chain Second Report and Order* adopted rules governing the maintenance, including updates, of the Covered List and tasked the Bureau with both publishing and maintaining it on the Commission's website in accordance with the Commission's rules.⁴ The Commission's rules require⁵ the Commission to place on the Covered List any communications equipment or service if a source enumerated in the Secure Networks Act determines that the equipment or service poses an unacceptable risk to the national security of the United States and if the communications equipment or service is

¹ Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, § 2(a), (d), 133 Stat. 158, 158-59 (2020) (codified as amended at 47 U.S.C. §§ 1601-1609) (Secure Networks Act).

² *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Second Report and Order, 35 FCC Rcd 14284, 14375-76 (2020) (*Supply Chain Second Report and Order*) (adopting 47 CFR §§ 1.50002, 1.50003).

³ 47 U.S.C. § 1601(d)(1); 47 CFR § 1.50003(a).

⁴ See *Supply Chain Second Report and Order*, 35 FCC Rcd at 14311-25, paras. 57-92.

⁵ The Commission found that if a determination by an enumerated national security agency, or intergovernmental agency with national security expertise, "indicates that a specific piece of equipment or service poses an unacceptable risk to the national security of the United States and the security and safety of United States persons, the Commission will automatically include this determination on the Covered List." *Supply Chain Second Report and Order*, 35 FCC Rcd at 14320, para. 80. The Commission took this approach "because of the plain language in section 2(b)(2)(C) which lists, among other equipment or service capabilities mandating inclusion on the Covered List, whether the equipment or service poses an unacceptable risk to the national security of the United States or the security and safety of United States persons. If an enumerated source has already performed this analysis as part of its determination, the only action we need take is to incorporate this determination onto the Covered List." *Id.* The Commission, in adopting the rules, interpreted Congress's use of the words "shall place" to mean it had no discretion to disregard determinations from these enumerated sources. *Supply Chain Second Report and Order*, 35 FCC Rcd at 14312, para. 59.

capable of posing an unacceptable risk to the national security of the United States.⁶

The Bureau has identified two determinations that meet the statutory criteria for additions to the Covered List. Both determinations were reflected in letters submitted to the Commission on behalf of interested parties of the Executive Branch (Executive Branch entities) by the Department of Commerce's National Telecommunications and Information Administration (NTIA)—one letter concerns Pacific Networks Corp. ("PacNet") and its wholly-owned subsidiary ComNet (USA) LLC ("ComNet") (collectively "PacNet/ComNet"),⁷ and the other concerns China Unicom (Americas) Operations Limited ("China Unicom").⁸ The letters explain how PacNet/ComNet and China Unicom, respectively, are subject to the exploitation, influence and control of the Chinese government, and the national security risks associated with such exploitation, influence, and control.⁹ In recent letters to the Commission, the Department of Justice (DoJ), in coordination with and with the concurrence of the Department of Defense (DoD), confirms that the Executive Branch's views in the PacNet/ComNet Executive Branch Letter and the CUA Executive Branch Letter, respectively, reflect a determination that the international section 214 services provided by PacNet/ComNet and China Unicom involve communications services that pose "an unacceptable risk to the national security of the United States or the security and safety of United States persons" under section 2 of the Secure Networks Act—thus requiring the addition of these services to the Covered List.¹⁰ Accordingly, by this Public Notice, we update the Covered List.

With respect to PacNet/ComNet, the Executive Branch entities found that the Government of the People's Republic of China's (PRC) majority ownership and control of PacNet and its wholly-owned subsidiary ComNet through parent company CITIC Group Corporation, combined with Chinese intelligence and cybersecurity laws, raise concerns that PacNet/ComNet will be forced to comply with Chinese government requests for communications intercepts, without the ability to challenge such requests.¹¹ The Executive Branch entities also found that PacNet/ComNet's interconnections to U.S. telecommunications networks and customers present opportunity for exploitation by the Chinese government to conduct or to increase economic espionage and collect intelligence against the United States, or otherwise provide a strategic capability to target, collect, alter, block, and re-route network traffic.¹² Additionally, based on the Executive Branch entities' finding that no further mitigation

⁶ 47 CFR § 1.50002; *see also* 47 U.S.C. §§ 1601(b)(1), 1601(b)(2)(C), 1601(c).

⁷ Letter from Kathy Smith, Chief Counsel, National Telecommunications and Information Administration, U.S. Department of Commerce, to Denise Coca, Chief, Telecommunications and Analysis Division, FCC International Bureau at 1 (Nov. 16, 2020) (on file in GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199) (PacNet/ComNet Executive Branch Letter). The interested Executive Branch entities include the Department of Justice, Department of Homeland Security, Department of Defense, Department of Commerce, Department of the Treasury, Department of State, Office of Management and Budget, Office of the U.S. Trade Representative, General Services Administration, and Council of Economic Advisers. *See* PacNet/ComNet Executive Branch Letter at 1 n.3.

⁸ Letter from Kathy Smith, Chief Counsel, National Telecommunications and Information Administration, U.S. Department of Commerce, to Denise Coca, Chief, Telecommunications and Analysis Division, FCC International Bureau at 1 (Nov. 16, 2020) (on file in GN Docket No. 20-110, File Nos. ITC-214-20020728-00361, ITC-214-20020724-00427) (CUA Executive Branch Letter).

⁹ *See* PacNet/ComNet Executive Branch Letter; CUA Executive Branch Letter.

¹⁰ Letter from Lee Licata, Deputy Section Chief for Telecom and Supply Chain, Foreign Investment Review Section, National Security Division, U.S. Department of Justice, to Marlene H. Dortch, Secretary, Federal Communications Commission (Sept. 15, 2022) (on file in WC Docket No. 18-89, ET Docket No. 21-232, EA Docket No. 21-233). In its letters, DoJ also notes that the PacNet/ComNet and China Unicom Executive Branch Letters represented the view of DoD, which qualifies as an "appropriate national security agency" authorized to make determinations pursuant to section 2 of the Secure Networks Act. *Id.* at 2.

¹¹ PacNet/ComNet Executive Branch Letter at 6.

¹² PacNet/ComNet Executive Branch Letter at 10.

measures by PacNet/ComNet would fully eliminate the risks to American law enforcement and national security,¹³ the Executive Branch entities have determined that services provided by PacNet/ComNet pose an unacceptable risk to the national security of the United States and its people.

With respect to China Unicom, the Executive Branch entities found that the United States national security environment, including increased concern about malicious cyber activities taken at the direction of the Government of the PRC, has changed significantly since 2002, when the Commission certified the international section 214 authorization of China Unicom to provide international common carrier services;¹⁴ that China Unicom's status as a wholly-owned subsidiary of a PRC state-owned enterprise firmly places it under the exploitation, control, and influence of the Chinese government;¹⁵ that China Unicom has continuing and ongoing commercial relationships with Chinese entities accused of engaging in activities contrary to American national security and economic interests;¹⁶ and that China Unicom's American operations provide opportunity to facilitate Chinese cyber activities including economic espionage, disruption and misrouting of American communications traffic, and access to U.S. records and other sensitive data.¹⁷ Accordingly, based on these findings, the Executive Branch entities have determined that services provided by China Unicom associated with its international section 214 authorization pose a substantial and unacceptable risks to the national security of the United States and its people.

The inclusion of these services on the Covered List extends both to subsidiaries and affiliates of the named entities.

Consistent with the Secure Networks Act and the Commission's rules, the Bureau will update this list upon becoming aware of any equipment or service that satisfies the criteria established in section 2 of the Secure Networks Act and section 1.50002 of the Commission's rules.

For further information, please contact Zenji Nakazawa, Associate Bureau Chief, Public Safety and Homeland Security Bureau at or Zenji.Nakazawa@fcc.gov.

– FCC –

¹³ PacNet/ComNet Executive Branch Letter at 10-11.

¹⁴ CUA Executive Branch Letter at 2, 2-6.

¹⁵ CUA Executive Branch Letter at 2, 6-11.

¹⁶ CUA Executive Branch Letter at 2-9.

¹⁷ CUA Executive Branch Letter at 2, 34-35.

APPENDIX

COVERED LIST (Updated September 20, 2022)*†

Covered Equipment or Services*	Date of Inclusion on Covered List
Telecommunications equipment produced or provided by Huawei Technologies Company , including telecommunications or video surveillance services produced or provided by such entity or using such equipment.	March 12, 2021
Telecommunications equipment produced or provided by ZTE Corporation , including telecommunications or video surveillance services provided or provided by such entity or using such equipment.	March 12, 2021
Video surveillance and telecommunications equipment produced or provided by Hytera Communications Corporation , to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services produced or provided by such entity or using such equipment.	March 12, 2021
Video surveillance and telecommunications equipment produced or provided by Hangzhou Hikvision Digital Technology Company , to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services produced or provided by such entity or using such equipment.	March 12, 2021
Video surveillance and telecommunications equipment produced or provided by Dahua Technology Company , to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services produced or provided by such entity or using such equipment.	March 12, 2021
Information security products, solutions, and services supplied, directly or indirectly, by AO Kaspersky Lab or any of its predecessors, successors, parents, subsidiaries, or affiliates.	March 25, 2022
International telecommunications services provided by China Mobile International USA Inc. subject to section 214 of the Communications Act of 1934.	March 25, 2022
Telecommunications services provided by China Telecom (Americas) Corp. subject to section 214 of the Communications Act of 1934.	March 25, 2022
International telecommunications services provided by Pacific Networks Corp. and its wholly-owned subsidiary ComNet (USA) LLC subject to section 214 of the Communications Act of 1934.	September 20, 2022
International telecommunications services provided by China Unicom (Americas) Operations Limited subject to section 214 of the Communications Act of 1934.	September 20, 2022

*The inclusion of producers or providers of equipment or services identified on this list should be read to include the subsidiaries and affiliates of such entities.

†Where equipment or services on the list are identified by category, such category should be construed to include only equipment or services capable of the functions outlined in sections 2(b)(2)(A), (B), or (C) of the Secure and Trusted Communications Networks Act of 2019, 47 U.S.C. § 1601(b)(2)(A)-(C).