PUBLIC NOTICE

Federal Communications Commission
45 L Street NE
Washington, DC 20554

News Media Information 202-418-0500
Internet: www.fcc.gov
TTY: 888-835-5322

DA 21-1572
Released: December 17, 2021

WIRELESS TELECOMMUNICATIONS BUREAU PROVIDES GUIDANCE FOR FILING CONTRABAND INTERDICTION SYSTEM CERTIFICATION APPLICATIONS AND SELF-CERTIFICATIONS

GN Docket No. 13-111

I. INTRODUCTION

1. As directed by the Commission in the *Second Report and Order* in the above-referenced proceeding,[1] the Wireless Telecommunications Bureau (Bureau), through this *Public Notice*, provides guidance to stakeholders and additional details on the process for obtaining approval of a Contraband Interdiction System (CIS) for use in the submission of qualifying requests for the disabling of contraband wireless devices in correctional facilities.

2. In the *Second Report and Order*, the Commission adopted a framework requiring the disabling of contraband wireless devices detected in correctional facilities upon satisfaction of certain criteria.[2] The process of certifying CISs for this purpose consists of two phases: (1) CIS applicants submit certification applications to the Bureau describing the legal and technical qualifications of the systems; and (2) CIS applicants perform on-site testing of approved CISs at individual correctional facilities and file self-certifications with the Bureau confirming that the testing at a specific correctional facility is complete and was successful.[3] After both phases are complete, designated correctional facility officials (DCFOs) are authorized to submit qualifying requests to wireless providers to disable contraband devices located at a CIS approved/tested correctional facility.

3. Note that this framework and CIS authorization process is separate and distinct from, and does not replace, the process through which solutions providers historically have obtained authorization to operate CISs in correctional facilities by entering into lease arrangements with wireless providers. Here, we provide guidance for applicants regarding the specific CIS authorization framework and authorization process required where stakeholders seek CIS certification to take the additional step of relying on newly adopted Commission rules (when effective) to request disabling of contraband wireless devices identified through CIS use. We also provide details regarding providing required notice of testing to wireless providers; the filing of self-certifications after site testing at each operational location; service of copies of self-certifications on certain parties; the filing of any objections to the self-certifications; and required system recertification after three years. Further, this *Public Notice* provides additional detail regarding the certification and listing of DCFOs to ensure that the parties submitting disabling requests have the

[1] *See In the Matter of Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, GN Docket No. 13-111, Second Report and Order and Second Further Notice of Proposed Rulemaking, FCC 21-82, at 9, 11, 15, 25, paras. 20, 24, 35, 59 (rel. July 13, 2021) (*Second Report and Order*); *see also In the Matter of Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, GN Docket No. 13-111, Erratum (rel. Aug. 3, 2021).

[2] *See Second Report and Order* at 2, para. 2.

[3] *See id*. at 10-16, paras 22-38.

necessary authority to submit qualifying requests for contraband device disabling, as well as guidance for providing quarterly notice, if relevant, to the Contraband Ombudsperson of erroneously disabled wireless devices. In sum, the guidance is intended to encourage CIS applicants to include sufficient detail to permit the Bureau to make a determination that the CIS meets the Commission's certification requirements.

4. We remind stakeholders that the *Second Report and Order* contains new information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law No. 104-13, and therefore the Office of Management and Budget (OMB) must review and provide approval under section 3507(d) of the PRA before many of the adopted rules can take effect. The Bureau will issue a subsequent Public Notice announcing the date on which we will begin accepting initial CIS certification applications and requests to become DCFOs.

A. CIS Certification Applications

5. The first phase of the disabling process requires a CIS applicant to submit a certification application to the Bureau describing the legal and technical qualifications of the system that the applicant seeks to use as the basis for qualifying requests for contraband device disabling. Following approval, the Bureau will maintain a publicly available list of certified CISs at https://www.fcc.gov/wireless/bureau-divisions/mobility-division/contraband-wireless-devices.[4]

1. CIS Description

6. Pursuant to the *Second Report and Order*, to obtain CIS certification for ultimate use in submitting qualifying requests, a CIS applicant must submit an application to the Bureau for approval.[5] In Section 1 of the application, the applicant must demonstrate, at a minimum, that:

(1) *Equipment Authorization*: all radio transmitters used as part of the CIS have appropriate equipment authorizations pursuant to Commission rules, by providing a certification to that effect;

(2) *CIS Design/Methodology*: the CIS is designed and will be configured to locate devices solely within a correctional facility, and that the methodology to be used in analyzing data collected by the CIS is adequately robust to ensure that a particular wireless device is in fact located within a correctional facility. In this regard, applicants must also provide:

- a description of the scope and overall function of the system;
- a description of the system architecture and configuration with diagrams;
- a description of the hardware and its functions;
- a description of the software and its functions;
- a description of the steps required and preparations needed to implement the CIS at any correctional facility (e.g., site surveys, engineering design, installation, and optimization);
- a description of how the CIS, if so required, interacts with a wireless provider network;
- a description of data analysis techniques; and
- a description of the key performance factors that indicate successful operation, including the expected level of percentage accuracy in the rate of detection of

[4] *See id.* at 11, para. 25.

[5] *See id.* at 10, para. 23.

contraband devices vs. non-contraband devices using a relevant sample size (e.g., number of devices to be observed and the length of observation period) and the rationale for the expectation;

(3) *Data Security*: the CIS will secure and protect all data collected and/or information produced as part of its intended use, including a description of the types of data the CIS collects, whether the data is retained and for how long, and how the data is stored and protected;

(4) *911 Calls*: the CIS will not interfere with emergency 911 calls, including a description of the methodology used for allowing emergency 911 calls to be permitted; and

(5) *Spectrum/Network Access Agreement*: the applicant is aware that a CIS may require a spectrum or network access agreement (e.g., a spectrum leasing arrangement or roaming agreement) to be authorized to operate by stating and describing whether the CIS requires such an agreement to operate.[6]

2. CIS Test Plan

7. In the *Second Report and Order*, the Commission stated that the application for CIS certification must include a test plan that can be adapted to the circumstances of each planned deployment at a specific correctional facility.[7] The purpose of the test plan is to evaluate a CIS's ability to identify contraband wireless devices within a correctional facility, while avoiding identifying devices located outside of the correctional facility, and also permitting emergency 911 calls. The test plan must be designed to demonstrate, when applied at a specific correctional facility, the CIS operator's predicted system accuracy rate and that emergency 911 calls are unaffected. We therefore remind applicants that the test plan must address the full scope of intended operation and, if approved, must be implemented to evaluate the CIS at a specific correctional facility(ies). Further, to ensure system effectiveness, we anticipate that an applicant would indicate that all site-based testing is to be conducted in real-time, live conditions.

8. An applicant must provide a test plan in Section 2 of its CIS application that includes, at a minimum:

(1) A proposed evaluation of the functions that the CIS will perform;

(2) A description of the testing device(s) placement and the number of testing devices that will be used at the correctional facility(ies);

(3) A demonstration of how the placement and number of testing devices are sufficient to evaluate the CIS as the applicant intends to market and operate the system;

(4) A demonstration that the testing will be randomized, and an explanation of why the number of devices and trials are statistically significant;

(5) A description of the data to be collected, including the number of devices correctly and incorrectly identified and/or intercepted as contraband, and the number of emergency 911 calls made and impacted; and

(6) the precise method to be used for calculating the accuracy of the CIS and verifying that emergency 911 calls are unaffected.

B. CIS Certification Application Filing Process

9. The CIS certification application must be signed by a duly authorized representative of the applicant; for example, by one of the partners if the applicant is a partnership; or by an officer,

[6] *Id*. We note that, at this initial stage, an applicant is not required to have reached such an agreement.

[7] *Second Report and Order*, at 12, para. 27.

director, or duly authorized employee, if the applicant is a corporation; or by a duly elected or appointed official who is authorized to do so under the laws of the applicable jurisdiction if the applicant is a government entity.[8] We remind applicants that their applications must contain truthful and accurate information, and we therefore require a CIS applicant to include a declaration in compliance with Commission rule section 1.16.[9]

10. *CIS Certification Application Filing Procedures.* CIS applications filed pursuant to Commission rule section 20.23[10] must be filed using the Commission's Electronic Comment Filing System (ECFS). *See Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998). All such filings must refer to **GN Docket 13-111**. Such CIS applications must be filed on or after the date indicated in a future Bureau Public Notice. In addition, CIS applicants may request confidential treatment of information contained in their applications consistent with section 0.459 of the Commission's rules.[11] We direct prospective CIS applicants to review the Commission's previous guidance on the submission of confidential information, which was released in March 2020.[12] Recognizing that one purpose of the certification process is to "enable targeted industry review of solutions by allowing interested stakeholders to provide feedback on the application for certification, including the proposed test plan,"[13] we remind CIS applicants requesting confidential treatment to seek protection only of relevant portions of the application (e.g., those that are considered proprietary or contain sensitive material related to law enforcement).[14]

11. *Stakeholder Review of CIS Certification Applications.* As stated in the *Second Report and Order*, stakeholders will have an opportunity to review and comment on the CIS certification applications prior to testing or deploying at a correctional facility.[15] CIS applications found to be complete will be placed on public notice for review and comment. Stakeholders seeking review of confidential filings are required to follow the procedures set forth in section 0.461 of the Commission's rules.[16]

II. CIS SITE-BASED TESTING AND SELF-CERTIFICATION

12. A CIS operator—which could be a CIS solutions provider, or a DCFO or other responsible party that deploys its own CIS at a correctional facility—seeking to use the CIS to submit qualifying requests for disabling must test a certified CIS, based on the previously approved test plan, at each location where it intends to operate.[17] Thereafter, in order for the system to be used in the submission of qualifying requests at a specific correctional facility, the CIS operator must file a self-certification with the Bureau indicating that the testing at that correctional facility is complete and was successful, as described below.[18]

---

[8] *See* 47 CFR § 1.917.

[9] *See* 47 CFR § 1.16.

[10] *See id*.

[11] *See* 47 CFR § 0.459 (detailing procedures to request withholding materials from public inspection).

[12] *See FCC Provides Instructions Regarding Submission of Confidential Materials*, Public Notice, 35 FCC Rcd 2973 (2020).

[13] *See Second Report and Order*, at 12, para. 28.

[14] *See* 47 CFR § 0.459; *see also Second Report and Order*, at 11, para. 24.

[15] *Second Report and Order*, at 11, 12, paras. 24, 27.

[16] *See id.* at § 0.461 (detailing procedures for inspecting materials not routinely available for public inspection).

[17] *See Second Report and Order*, at 14, para. 32.

[18] *See infra* para 14; *see also Second Report and Order*, at 14, para. 34.

13. *Service of Notice of Testing Procedures*. In the *Second Report and Order*, the Commission stated that prior to initiating testing at a correctional facility, the CIS operator must serve notice of the testing on all relevant wireless providers[19] and provide each such provider a reasonable opportunity to participate in the tests.[20] We require CIS operators to serve notice, in accordance with Commission rule section 1.47,[21] of the testing on all relevant wireless providers by email no later than seven business days before the date that testing will begin. The notice must include, at a minimum, the following information: (1) testing start and end date; (2) testing location; (3) testing parameters; and (4) contact information.

14. *CIS Operator Self-Certification Filing Procedures.* Following completion of successful CIS testing, to be eligible for use in conjunction with qualifying requests for disabling, the CIS operator must file a self-certification that: (1) identifies the correctional facility where it seeks to deploy; (2) attests that applicable federal or state criminal statutes prohibit the possession or operation of contraband devices within the correctional facility (and includes the applicable federal or state criminal statutory provision); (3) describes the results of the certified CIS on-site tests conducted at the correctional facility; (4) attests that the on-site testing was performed consistent with the approved test plans for the certified CIS and that the CIS deployment minimizes the risk of disabling a non-contraband device; (5) identifies whether any relevant wireless providers participated in the testing and provides proof that the relevant wireless providers were given notice regarding the testing and a reasonable opportunity to participate; and (6) includes proof of any spectrum and/or network access agreement (e.g., a spectrum leasing arrangement and/or roaming agreement) required to be authorized to operate at this correctional facility and/or for the system to function effectively.[22] The self-certification submitted by a CIS operator must include a certification consistent with Commission rule section 1.16 and must also be accompanied by an attestation from the DCFO verifying that all information contained in the self-certification is true and accurate.[23] We require CIS operators to serve notice on all relevant wireless providers, in accordance with Commission rule section 1.47,[24] of the filing of the self-certification.

15. Prospective CIS operators must file CIS self-certifications using the Commission's ECFS. *See Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998). All such filings must refer to **GN Docket 13-111**.

16. *Wireless Providers Filing Objections to CIS Self-Certifications Procedures*. In the *Second Report and Order*, the Commission afforded wireless providers five business days from the certification filing date to submit objections to the Bureau, and provided that any such objections must be served on the DCFO and the CIS operator.[25] Absent objections, the DCFO may submit qualifying requests to wireless providers beginning on the sixth business day after the filing of the self-certification with the Bureau. If a timely objection is submitted, the DCFO may not submit qualifying requests until the Bureau addresses the objection. The Commission also clarified that a wireless provider may submit

[19] The Commission defined relevant wireless providers as any wireless provider holding a spectrum license that: (1) authorizes operation on the frequencies on which the CIS seeks to detect contraband use; and (2) authorizes service in the geographic area (e.g., census tract, county, PEA, EA, CMA, REAG) within which the correctional facility is located.

[20] *Second Report and Order*, at 14-15, para. 33 (to be codified at 47 CFR § 20.23(b)(3)(i) (site-based testing)).

[21] 47 CFR § 1.47.

[22] *Second Report and Order*, at 15, para. 34 (to be codified at 47 CFR § 20.23(b)(3)(ii) (self-certification)).

[23] *Second Report and Order*, at 15, para. 34.

[24] 47 CFR § 1.47.

[25] *Second Report and Order*, at 15, para. 35 (to be codified at 47 CFR § 20.23(b)(4) (submitting objections)).

an objection to the Bureau after the five-day period lapses but must nonetheless act on qualifying requests during the pendency of the objection.[26]

17. Wireless providers must file any objections to self-certifications through ECFS in **GN Docket No. 13-111**. In addition, in accordance with Commission rule section 1.47,[27] wireless providers must serve notice of the objection on the DCFO and the CIS operator when submitting the objection via ECFS.

18. *Certified CIS List.* After review of the CIS certification applications and self-certifications, the Commission will update its website regularly to include a list of certified CISs. In addition, the Commission's website will include, for each certified CIS, those correctional facilities where the system can be used in the submission of qualifying requests which indicates the system has been tested and self-certified for operational readiness and any timely objections have been resolved in favor of the CIS applicant.[28] The list will be posted at https://www.fcc.gov/wireless/bureau-divisions/mobility-division/contraband-wireless-devices.

19. *Recertification Procedures.* At least every three years after the initial self-certification, CIS operators seeking to maintain the ability to submit qualifying requests through a DCFO for contraband device disabling must retest their systems and recertify them for continued CIS accuracy.[29] Recertifications must comply with the same rules and filing instructions that apply to the initial self-certification as described in this *Public Notice* and the Commission's rules.[30]

III. DESIGNATED CORRECTIONAL FACILITY OFFICIAL REQUIREMENTS

20. In the *Second Report and Order*, the Commission adopted requirements for qualifying DCFOs to ensure that parties making disabling requests have the necessary authority and accountability to safeguard the integrity of the contraband device identification and disabling process.[31] Specifically, the Commission required that qualifying disabling requests be submitted by an official of the state, local, or federal government entity responsible for administration and oversight of the relevant correctional facility.[32] We will announce the date on which the Bureau will begin accepting requests from prospective DCFOs in a future Public Notice following OMB approval of the Commission's rules that are subject to the PRA. However, we take the opportunity in this Public Notice to outline the process to be used for such submissions to provide advance notice of the requirements. Any person meeting the DCFO definition that seeks authority to submit qualifying requests must send a letter, addressed to the Commission's Contraband Ombudsperson, signed by the relevant state attorney general or, if a federal correctional facility, the relevant Bureau of Prisons Regional Director, that provides the individual's name, official government position, and a list of correctional facilities over which the individual has oversight and management authority.[33] Specifically, the letter should be addressed to Charles Mathias, Contraband Ombudsperson, Federal Communications Commission, 45 L Street, NE, Washington, DC 20554. Consistent with the Privacy Act,[34] by submitting this letter, the individual seeking DCFO

[26] *Second Report and Order*, at 15, para. 35.

[27] 47 CFR § 1.47(b), (f) ("[w]here any person is required to serve any document filed with the Commission, service shall be made by that person or by his representative on or before the day on which the document is filed").

[28] *Second Report and Order*, at 11, para. 25 (to be codified at 47 CFR § 20.23(b)(3)(ii)(H) (submitting objections)).

[29] *Second Report and Order,* at 15, para. 36.

[30] *Second Report and Order*, at 15, para. 36 (to be codified at 47 CFR § 20.23(b)(5) (recertification)).

[31] *See Second Report and Order,* at 8, para. 17.

[32] *Id.* at 8, para. 19.

[33] *Id*. at 9, para. 20.

[34] 5 U.S.C. § 552a.

designation consents to their name, title, and related correctional facilities, as described in this paragraph, being made publicly available on the Commission's website. To facilitate and expedite the process for all parties, we direct prospective DCFOs to file the required letter via ECFS and refer to **GN Docket No. 13-111**.

21. If the Commission confirms a DCFO's qualifications, it will add the DCFO to a list of approved DCFOs authorized to transmit qualifying disabling requests on the Commission's website. The list will be posted at https://www.fcc.gov/wireless/bureau-divisions/mobility-division/contraband-wireless-devices.

22. *Notice of Erroneously Disabled Devices*. Pursuant to the *Second Report and Order*, DCFOs must provide notice to the Contraband Ombudsperson of the number of erroneously disabled devices on a quarterly basis at the end of any quarter during which a device disabling was reversed.[35] Specifically, DCFOs required to provide this notice should submit a letter with the required information addressed to Charles Mathias, Contraband Ombudsperson, Federal Communications Commission, 45 L Street, NE, Washington, DC 20554. We direct DCFOs to file the required letter via ECFS and refer to **GN Docket No. 13-111**.

IV. CONTACT INFORMATION

23. Questions regarding this *Public Notice* may be directed to Melissa Conway, Attorney Advisor, Wireless Telecommunications Bureau, Mobility Division at (202) 418-2887 or Melissa.conway@fcc.gov.

-FCC-

[35] *Second Report and Order*, at 25, para. 59 (to be codified at 47 CFR § 20.23(c)(4)(v) (notice of reversals)). A licensee may reverse a disabled wireless device if it determines that the wireless device was identified erroneously as contraband. The licensee must promptly inform the DCFO of the erroneously identified wireless device. *See id*. at 24-25, paras. 57-59.