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 23-547
Released: June 23, 2023

WIRELESS TELECOMMUNICATIONS BUREAU APPROVES FIVE CONTRABAND INTERDICTION SYSTEM CERTIFICATION APPLICATIONS UNDER PHASE ONE OF THE AUTHORIZATION PROCESS

GN Docket No. 13-111

I. INTRODUCTION

1. With this Public Notice, the Wireless Telecommunications Bureau (WTB or Bureau) approves five Contraband Interdiction System (CIS) certification applications filed, respectively, by: CellBlox Acquisitions, LLC;[1] ShawnTech Communications, Inc.;[2] Tecore Networks;[3] SOC, LLC;[4] and OmniProphis Corporation[5] (collectively, the Five CIS Applications), subject to the conditions described below. Each of the Five CIS Applications was filed under phase one of the Commission's two-phase process for certifying CIS for use in the submission of qualifying requests to disable contraband wireless devices in correctional facilities.

2. Approval of the Five CIS Applications allows each referenced CIS operator to market and sell its CIS as described in its respective application and supplement, and begin phase two testing. The referenced CIS operators may begin using their CISs in conjunction with any Designated

[1] Application of CellBlox Acquisitions, LLC for Certification of Contraband Interdiction System Under 47 CFR Section 20.23, GN Docket No. 13-111 (filed Aug. 9, 2022) (CellBlox CIS Application); Supplement to Application of CellBlox Acquisitions, LLC for Certification of Contraband Interdiction System under 47 CFR Section 20.23, GN Docket No. 13-111 (filed Oct. 31, 2022) (CellBlox CIS Supplement).

[2] ShawnTech Communications, Inc., CIS Certification Application, GN Docket No. 13-111 (filed Aug. 16, 2022) (ShawnTech CIS Application); ShawnTech Communications, Inc., CIS Certification Application Response, GN Docket No. 13-111 (filed Oct. 26, 2022) (ShawnTech CIS Supplement).

[3] Application of Tecore Networks for Certification of Contraband Interdiction System Under 47 CFR Section 20.23, GN Docket No. 13-111 (filed Aug. 22, 2022) (Tecore CIS Application); Letter from Carli Rae Bernal, Vice President, Tecore Networks, to Roger Noel, Mobility Division Chief, FCC, GN Docket No. 13-111 (filed Nov. 7, 2022) (Tecore CIS Supplement).

[4] Application of SOC, LLC for Certification of Contraband Interdiction System Under 47 CFR 20.23, GN Docket No. 13-111 (filed Nov. 3, 2022) (SOC CIS Application); Letter from Travis Berrier, Senior Director, SOC, LLC, to Roger Noel, Mobility Division Chief, FCC, GN Docket No. 13-111 (filed Jan. 23, 2023) (SOC CIS Supplement); Letter from Marjorie K. Conner, Counsel to SOC, LLC, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 13-111 (filed Jan. 23, 2023) (*SOC ex parte*).

[5] Application of OmniProphis Corporation for Certification of Contraband Interdiction System Under 47 CFR Section 20.23, GN Docket No. 13-111 (filed Nov. 30, 2022) (OmniProphis CIS Application); Letter from Joseph S. Noonan, CEO, OmniProphis Corporation, to Roger Noel, Mobility Division Chief, FCC, GN Docket No. 13-111 (filed Jan. 24, 2023) (OmniProphis CIS Supplement).

Correctional Facility Official's (DCFO's)[6] submission of qualifying requests for contraband wireless device disabling only after successful completion of the phase two testing and self-certification process.

II. BACKGROUND

3. 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.[7] The process of certifying CIS 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 certified CISs at individual correctional facilities and file self-certifications with the Bureau confirming that the testing at a specific correctional facility was completed successfully.[8] Following WTB review and approval of the phase one CIS certification applications that meet applicable requirements, stakeholders using certified CISs may begin phase two on-site testing at individual correctional facilities. After both phases are complete, and the period for filing objections has lapsed,[9] DCFOs are authorized to submit qualifying requests to wireless providers to disable contraband devices located at a CIS approved/tested correctional facility.

4. The Bureau began accepting CIS certification applications on May 3, 2022,[10] and received the Five CIS Applications.[11] Each applicant filed a supplement to its Certification Application during the period from October 2022 to January 2023. On March 24, 2023, the Bureau issued a Public Notice announcing that each of the Five CIS Applications had been found complete and inviting stakeholders to review and file comments on the applications.[12] CTIA and T-Mobile filed generally supportive comments for CIS certification and did not oppose the approval of the Five CIS Applications.[13]

---

[6] *See* 47 CFR § 20.3 (defining a Designated Correctional Facility Official); *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, 36 FCC Rcd 11813, 11818-21, paras. 12-20 (2021) (*Second Report and Order*); *see also Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, GN Docket No. 13-111, Erratum (rel. Aug. 3, 2021).

[7] *See Second Report and Order*, 36 FCC Rcd at 11814, para. 2.

[8] *See Second Report and Order*, 36 FCC Rcd at 11821-23, paras. 22-38.

[9] *See* 47 CFR § 20.3(c) (absent objections from a wireless provider . . . the DCFO may submit a qualifying request to a wireless provider beginning on the sixth business day after the later of the self-certification filing or actual service . . .).

[10] *Wireless Telecommunications Bureau Begins Accepting Contraband Interdiction System Certification Applications and Designated Correctional Facility Official Requests*, GN Docket No. 13-111, Public Notice, DA 22-475 (WTB 2022).

[11] CellBlox CIS Application; ShawnTech CIS Application; Tecore CIS Application; SOC CIS Application; OmniProphis CIS Application.

[12] *Wireless Telecommunications Bureau Seeks Comment on Five Contraband Interdiction System Certification Applications*, GN Docket No. 13-111, Public Notice, DA 23-224 (WTB 2023). The Bureau issued a Protective Order specifying procedures for Stakeholders seeking to review the confidential filings. *See Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, GN Docket No. 13-111, Protective Order, DA 23-223 (WTB 2023).

[13] Comments of CTIA on Five Contraband Interdiction System Certification Applications, GN Docket No. 13-111, File Nos. 0001, 0002, 0003, 0004, 0005 (rec. Apr. 24, 2023) (CTIA Comments); Comments of T-Mobile USA, Inc., GN Docket No. 13-111, File Nos. 0001, 0002, 0003, 0004, 0005 (rec. Apr. 24, 2023) (T-Mobile Comments). CTIA notes that "mobile MAS deployments as a group raise . . . questions about accuracy" and the Commission should be cognizant of this "going forward as new applications are filed." CTIA Comments at 3-4. T-Mobile reviewed the applications and states that it "supports the Commission's certification of a range of CIS operations designed to meet different needs, including both fixed and mobile CIS." T-Mobile Comments at 2.

III. APPROVAL OF PHASE ONE CIS APPLICATIONS

5. After careful review of each application and the record, we find that the CIS applications filed by CellBlox, ShawnTech, Tecore, SOC, and OmniProphis, respectively, satisfy the eligibility criteria and application requirements, as specified in section 20.23 of the Commission's rules, the *Second Report and Order*, and the *Guidance Public Notice*.[14] As directed by the Commission in the *Second Report and Order*, the Bureau issued the *Guidance Public Notice* to provide guidance on the information required for inclusion in a CIS certification application and on the procedures for the submission of an application.[15] Specifically, phase one of the CIS certification application process requires an applicant to describe the legal and technical qualifications of, and provide a test plan for, the system that the applicant seeks to use as the basis for qualifying requests for contraband device disabling.[16] We briefly discuss each of the phase one application requirements in turn below.

6. *CIS Certification Application Description*.[17] We find that the Five CIS Applications sufficiently described the legal and technical qualifications of its CIS. Further, in accordance with Commission rules, the Five CIS Applications demonstrated 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;[18]

(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, each CIS applicant also provided:

- 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,

[14] *See* 47 CFR § 20.23; *Second Report and Order*, 36 FCC Rcd at 11821-23, paras. 22-38; *Wireless Telecommunications Bureau Provides Guidance for Filing Contraband Interdiction System Certification Applications and Self-Certifications*, GN Docket No. 13-111, DA 21-1572, 2-3, paras. 6-8 (WTB 2021) (*Guidance Public Notice*).

[15] *Guidance Public Notice* at 2-4, paras. 5-6, 9-10.

[16] *Guidance Public Notice* at 2-4, paras. 5-10.

[17] *See* 47 CFR § 20.23(b)(1)(i)-(vi) (application requirements); *Second Report and Order*, 36 FCC Rcd at 11821, para. 23; *Guidance Public Notice* at 2-3, para. 6.

[18] CellBlox CIS Application at 5; ShawnTech CIS Application at 1; Tecore CIS Application at 18; Tecore CIS Application, Exhs. A-B; SOC CIS Application at 3; OmniProphis CIS Application at 11.

including the expected level of percentage accuracy in the rate of detection of 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;[19]

(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;[20]

(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;[21] 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.[22]

7. *CIS Certification Application Test Plan.* We also find that the Five CIS Applications included a test plan that can be adapted to the circumstances of each planned deployment at a specific correctional facility, and adequately demonstrated that each CIS's overall methodology for system design and data analysis ensures, to the greatest extent possible, that only devices that are in fact contraband will be identified for disabling.[23] Specifically, each CIS applicant included:

(1) A proposed evaluation of the functions that the CIS will perform;[24]

(2) A description of the testing device(s) placement and the number of testing devices

[19] CellBlox CIS Application at 5-16; CellBlox CIS Supplement at 2-11; ShawnTech CIS Application at 2-10; ShawnTech CIS Supplement at 1-7; Tecore CIS Application at 18-29; Tecore CIS Supplement at 1-5; SOC CIS Application at 3-14; SOC CIS Supplement at 1-7; *SOC ex parte* at 3-9, 12-14; OmniProphis CIS Application at 11-16; OmniProphis CIS Supplement at 2-5. Each CIS applicant provided information regarding its CIS design and methodology for which it sought, in part, confidential treatment pursuant to Commission rule section 0.459, 47 CFR § 0.459.

[20] CellBlox CIS Application at 16-18; ShawnTech CIS Application at 10; Tecore CIS Application at 29-31; SOC CIS Application at 14-16; OmniProphis CIS Application at 16-18. Each CIS applicant provided information regarding its CIS data security methods for which it sought, in part, confidential treatment pursuant to Commission rule section 0.459, 47 CFR § 0.459.

[21] CellBlox CIS Application at 18; CellBlox CIS Supplement at 11-13; ShawnTech CIS Application at 10-11; Tecore CIS Application at 31-33; SOC CIS Application at 16; OmniProphis CIS Application at 19, 22; OmniProphis CIS Supplement at 4-5. Each CIS applicant provided information regarding its routing of 911 calls for which it sought, in part, confidential treatment pursuant to Commission rule section 0.459, 47 CFR § 0.459.

[22] CellBlox CIS Application at 18-19; ShawnTech CIS Application at 11; Tecore CIS Application at 34; SOC CIS Application at 16; OmniProphis CIS Application at 18; *see also* T-Mobile Comments at 2 (stating "it has entered into agreements with most of [the CIS applicants] to facilitate their access to spectrum licensed to T-Mobile, or its affiliates, in order to operate CIS within correctional facilities"). Tecore and OmniProphis each provided information regarding its spectrum/network access agreements for which it sought, in part, confidential treatment pursuant to Commission rule section 0.459, 47 CFR § 0.459.

[23] *See* 47 CFR § 20.23(b)(1)(vii) (application requirements); *Second Report and Order*, 36 FCC Rcd at 11822-23, paras. 26-27; *Guidance Public Notice* at 2-3, paras. 7-8.

[24] CellBlox CIS Application at 19-22; CellBlox CIS Supplement at 14-19; ShawnTech CIS Application at 11-12; ShawnTech CIS Supplement at 7-8; Tecore CIS Application at 35-37; SOC CIS Application at 17-22; *SOC ex parte* at 12-14; OmniProphis CIS Application at 18-19; OmniProphis CIS Supplement at 5-7. Each CIS applicant provided information regarding its CIS proposed functions for which it sought, in part, confidential treatment pursuant to Commission rule section 0.459, 47 CFR § 0.459.

that will be used at the correctional facility(ies);[25]

(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;[26]

(4) A demonstration that the testing will be randomized, and an explanation of why the number of devices and trials are statistically significant;[27]

(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;[28] and

(6) the precise method to be used for calculating the accuracy of the CIS and verifying that emergency 911 calls are unaffected.[29]

IV. CONCLUSION

8. Based on our review, we approve, subject to the conditions below, the Five CIS Applications in the public interest. Through the issuance of this Public Notice, CellBlox, ShawnTech, Tecore, SOC, and OmniProphis may market and sell their certified CISs as described in the respective Applications for ultimate use, following phase two testing, in obtaining information for the submission of qualifying requests for the disabling of contraband wireless devices.[30] The referenced entities may begin the phase two on-site testing of their CISs at individual correctional facilities as outlined in the *Second Report and Order* and more specifically in section 20.23 of the Commission's rules.[31] We remind all CIS operators receiving approval of their CIS Applications that they must file a self-certification following

[25] CellBlox CIS Application at 22-25; CellBlox CIS Supplement at 14-19; ShawnTech CIS Application at 11-12; ShawnTech CIS Supplement at 7-8; Tecore CIS Application at 37-38; SOC CIS Application at 16-19; SOC CIS Supplement at 7-8; OmniProphis CIS Application at 19. Each CIS applicant provided information regarding its CIS testing placement and number of testing devices for which it sought, in part, confidential treatment pursuant to Commission rule section 0.459, 47 CFR § 0.459.

[26] CellBlox CIS Application at 25; CellBlox CIS Supplement at 7, 14-19; ShawnTech CIS Application at 12-13; ShawnTech CIS Supplement at 7-8; Tecore CIS Application at 37-38; Tecore CIS Supplement at 5-6; SOC CIS Application at 20-21; SOC CIS Supplement at 7-8; OmniProphis CIS Application at 19. Each CIS applicant provided information regarding how the placement and number of testing devices are sufficient to evaluate the CIS for which it sought, in part, confidential treatment pursuant to Commission rule section 0.459, 47 CFR § 0.459.

[27] CellBlox CIS Application at 26; CellBlox CIS Supplement at 14-19; ShawnTech CIS Application at 13-14; ShawnTech CIS Supplement at 7-8; Tecore CIS Application at 38-39; SOC CIS Application at 20-21; SOC CIS Supplement at 7-8; OmniProphis CIS Application at 19-20. Each CIS applicant provided information regarding its data validation methodology for which it sought, in part, confidential treatment pursuant to Commission rule 0.459, 47 CFR § 0.459.

[28] CellBlox CIS Application at 26; CellBlox CIS Supplement at 14-19; ShawnTech CIS Application at 14; ShawnTech CIS Supplement at 7-9; Tecore CIS Application at 40; SOC CIS Application at 22-23; SOC CIS Supplement at 8-10; OmniProphis CIS Application at 20; OmniProphis CIS Application at 5-7. Each CIS applicant provided information regarding the description of the data to be collected by its CIS for which it sought, in part, confidential treatment pursuant to Commission rule section 0.459, 47 CFR § 0.459.

[29] CellBlox CIS Application at 26; CellBlox CIS Supplement at 14-19; ShawnTech CIS Application at 14-15; ShawnTech CIS Supplement at 7-9; Tecore CIS Application at 40-43; SOC CIS Application at 22; SOC CIS Supplement at 8-10; OmniProphis CIS Application at 20-21; OmniProphis CIS Application at 5. Each CIS applicant provided information regarding its method for calculating CIS accuracy for which it sought, in part, confidential treatment pursuant to Commission rule 0.459, 47 CFR § 0.459.

[30] *See* 47 CFR § 20.23(b)(2) (marketing and sales); *Second Report and Order*, 36 FCC Rcd at 11822, para. 25.

[31] *See* 47 CFR § 20.23(b)(3) (site-based testing and self-certification requirements); *see also Second Report and Order*, 36 FCC Rcd at 11821-23, paras. 22-38; *Guidance Public Notice* at 4-6, paras. 12-19.

completion of successful CIS testing.[32] The self-certifications must be filed using the Commission's Electronic Comment Filing System (ECFS) and must reference **GN Docket No. 13-111**.[33]

9. *Conditions.* This CIS certification application approval and each CIS operator's use of its certified CIS for the ultimate submission of qualifying requests is conditioned on the following:

1) Testing of the certified CIS and its subsequent operation and use to support qualifying requests must be as specifically described in that CIS operator's application and supplement as approved through this Public Notice;
2) A phase two testing self-certification, and a subsequently filed qualifying request, must be based upon information received from a certified CIS in deployed areas of an individual correctional facility where the CIS has been fully tested in real-time, live conditions consistent with the approved test plan;
3) The certified CIS must remain highly accurate regarding its:
   a) capability to identify only those devices physically located within the perimeter of operation; and
   b) ability to distinguish between contraband and non-contraband devices;
4) Approved CIS may be marketed and sold only to correctional facilities or entities that will provide contraband interdiction services to such facilities.

10. *Contact Information.* Questions regarding this *Public Notice* may be directed to Halie Peacher, Attorney Advisor, Wireless Telecommunications Bureau, Mobility Division at (202) 418-0514 or Halie.Peacher@fcc.gov.

-FCC-

[32] *See* 47 CFR § 20.23(b)(3) (site-based testing and self-certification requirements); *see also Guidance Public Notice* at 5, para. 14.

[33] *See Guidance Public Notice* at 5, para. 15; *see also Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998).