

**Section 20.23(b)(1), (3)-(5), (7); (c)(1)-(2), (3), (3)(iii)-(iv), (4)(i)-(ii), (v); and (d),
Contraband wireless devices in correctional facilities**

SUPPORTING STATEMENT

A. Justification:

1. Explain the circumstances that make the collection of information necessary.

The Federal Communications Commission (Commission) is seeking a three year extension from the Office of Management and Budget , of an information collection for the following of Commission rule section 20.23(b), *Contraband Interdiction System (CIS) authorization process*: paragraph (b)(1), *Application requirements*, paragraph (b)(3), *Site-based testing and self-certification requirements*, paragraph (b)(4), *Submitting objections*, paragraph (b)(5), *Recertification*, and paragraph (b)(7), *Records maintenance*; the following paragraphs of section 20.23(c), *Disabling contraband wireless devices*: paragraph (c)(1), *DCFO list*, paragraph (c)(2), *Qualifying request*, paragraph (c)(3), (3)(iii)-(iv), *Licensee actions upon receipt of a qualifying request*, (*Rejection of a qualifying request and timing*; *Customer outreach*; *Notification to the Designated Correctional Facility Official*); paragraph (c)(4)(i)-(ii), (v), *Reversals*; and paragraph (d) of section 20.23, *Notification to Managed Access System (MAS) operators of wireless provider technical changes*, in order to obtain another full 3 year clearance.

On February 3, 2022, the Commission received approval from OMB for the information collection under OMB Control Number 3060-1299. The information collection requirements under OMB Control Number 3060-1299 have not changed since the Commission's PRA request was approved by OMB on February 3, 2022. The Commission is requesting continued OMB approval for the information collection requirements that were approved in the Commission's past submission.

On July 13, 2021, the Commission released a Second Report and Order and Second Further Notice of Proposed Rulemaking, *Promoting Technological Solutions to Combat Contraband Wireless Devices in Correctional Facilities*, GN Docket No. 13-111, FCC 21-82, in which the Commission took further steps to facilitate the deployment and viability of technological solutions used to combat contraband wireless devices in correctional facilities. 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. The Commission further addressed issues involving oversight, wireless provider liability, and treatment of 911 calls. Finally, the Commission adopted rules requiring advance notice of certain wireless provider network changes to promote and maintain contraband interdiction system effectiveness.

In establishing rules requiring wireless providers to disable contraband wireless devices in correctional facilities and adopting a framework to enable designated correctional facility

**Section 20.23(b)(1), (3)-(5), (7); (c)(1)-(2), (3), (3)(iii)-(iv), (4)(i)-(ii), (v); and (d),
Contraband wireless devices in correctional facilities**

officials (DCFOs) relying on an authorized Contraband Interdiction System (CIS) to submit qualifying requests to wireless providers to disable contraband wireless devices in qualifying correctional facilities, the Commission found that a rules-based process will provide a valuable additional tool for departments of corrections to address contraband wireless device use. The framework includes a two-phase authorization process: (1) CIS applicants will submit applications to the Wireless Telecommunications Bureau (Bureau) describing the legal and technical qualifications of the systems; and (2) CIS applicants will perform on-site testing of approved CISs at individual correctional facilities and file a self-certification with the Commission. After both phases are complete, DCFOs will be authorized to submit qualifying requests to wireless providers to disable contraband devices using approved CISs at each correctional facility. In addition, the Commission adopted rules requiring wireless providers to notify certain types of CIS operators of major technical changes to ensure that CIS effectiveness is maintained. The Commission found that these rules will provide law enforcement with the tools necessary to disable contraband wireless devices, which, in turn, will help combat the serious threats posed by the illegal use of such devices.

Section 20.23(b)(1), (3)-(5) (7):

(b) *Contraband Interdiction System (CIS) authorization process.* The provisions in this section apply to any person seeking certification of a CIS authorized for use in the submission of qualifying disabling requests, whether operating a system that requires a license and is regulated as Commercial Mobile Radio Services (CMRS) or private mobile radio service (PMRS), or operating a passive system that does not require a license. The Wireless Telecommunications Bureau (Bureau) established, via public notice which was released in December 2021 (*CIS Guidance Public Notice*, GN Docket No. 13-111, DA 21-1572), the form and procedure for: CIS operators to file CIS certification applications, self-certifications, and periodic re-certification; CIS operators to serve on wireless providers notice of testing and copies of self-certification; and wireless providers to file objections to self-certifications, including required service on CIS operators and DCFOs.

The Commission found that the technical CIS certification requirements will help ensure that the systems for detecting contraband wireless devices are designed to support operational readiness and minimize the risk of disabling a non-contraband device. The Bureau will base each certification determination on a demonstration that the 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. The Commission found that requiring a description of the proposed test plan will ultimately promote efficient CIS deployment and will facilitate Commission review of the systems for operational readiness prior to actual deployment. Included among the public interest benefits are that the certification process will enable targeted industry review of solutions by allowing interested stakeholders to provide feedback on the application for certification, including the proposed test plan. And, the certification process will ensure a high level of CIS accuracy by requiring

**Section 20.23(b)(1), (3)-(5), (7); (c)(1)-(2), (3), (3)(iii)-(iv), (4)(i)-(ii), (v); and (d),
Contraband wireless devices in correctional facilities**

that CIS applicants submit detailed showings and representations establishing that the systems are designed to minimize the risk of disabling a non-contraband wireless device. The certification process should ensure that CISs are designed to minimize the risk of disabling a non-contraband device, while refraining from imposing additional burdens, such as requiring that CIS operators fully deploy or test the systems prior to obtaining CIS certification.

To further ensure that the CIS authorization is appropriate, wireless providers may submit objections to the Bureau within five business days from the certification filing date. In addition, to ensure ongoing accuracy and reliability of a given CIS at a particular facility, the Bureau requires re-certification every three years after the initial self-certification. The re-certification process requires the CIS operators to retest their systems and recertify them in accordance with the Commission's rules.

The Commission also found that requiring CIS operators to submit a self-certification following on-site testing will help ensure that qualifying requests identify contraband wireless devices accurately and in accordance with relevant legal authorities. The Commission also found it in the public interest to require that a self-certification include the fact that an applicable state or federal criminal statute prohibits the possession or operation of a contraband wireless device within the correctional facility where the CIS is deployed for use. Completion of the on-site testing and self-certification phase of the authorization process allows DCFOs to submit to wireless providers qualifying requests to disable contraband phones at that particular facility. Wireless providers are given an opportunity to object to the certification which further ensures an accurate process. In order to ensure the ongoing accuracy and reliability of a given CIS at a particular facility, the Commission found it appropriate to require periodic re-certification. The Commission found that requiring CIS operators to maintain records will support robust efforts to identify issues with CIS operations, resolve interference issues, and resolve complaints related to misidentification of contraband devices.

Section 20.23(c)(1)-(2):

(c) Disabling contraband wireless devices. A DCFO may request that a CMRS licensee disable a contraband wireless device that has been detected in a correctional facility by a CIS that has been certified in accordance with paragraph (b) of this section. Absent objections from a wireless provider, as described under paragraph (b)(4) of this section, 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, as described under paragraph (b)(3)(ii) of this section.

The Commission adopted requirements for qualifying DCFOs that will ensure parties making disabling requests have the necessary authority and accountability to safeguard the integrity of the contraband device identification and disabling process. The Commission adopted a process for certification of DCFOs that will provide certainty to wireless providers that disabling requests are duly authorized by the relevant federal, state, or local government

**Section 20.23(b)(1), (3)-(5), (7); (c)(1)-(2), (3), (3)(iii)-(iv), (4)(i)-(ii), (v); and (d),
Contraband wireless devices in correctional facilities**

entities. Individuals that seek to be recognized on the Commission's DCFO list must send a letter 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. The Commission found that these requirements for DCFOs eligible to send qualifying requests to wireless providers will ensure an efficient process that safeguards the integrity and accuracy of the disabling process.

The Commission concluded that adopting standardized information for qualifying requests will help expedite transmission and review of the request by the wireless provider, as well as reduce the administrative burden on DCFOs. By requiring that qualifying requests include specific information necessary for wireless providers to act upon the request without establishing a standardized form, the Commission provided DCFOs and wireless providers the flexibility to structure the format of the qualifying requests while meeting the goal of facilitating efficient contraband wireless device disabling. The Commission found that certifications are a simple and efficient mechanism for demonstrating that a DCFO has exercised the due diligence necessary to validate the accuracy of the information being sent to wireless providers. The DCFO must include this certification as part of a qualifying request to help ensure the accuracy of the disabling process. The Commission found that the requirement that contraband device activity be observed within the 30-day period prior to the date of the submission of a qualifying request appropriately balances various temporal interests.

A qualifying request must include a list of the contraband devices, with identifiers sufficient to uniquely describe the devices at both the subscription- and device-levels, to provide the wireless provider with the information necessary to prevent use of contraband devices on its network and on other wireless provider networks. The Commission's two-step authorization process ensures that a certified CIS can identify contraband devices with a high degree of certainty. This process should provide sufficient assurance that the devices listed in the qualifying request are contraband devices that are being used unlawfully. By requiring, however, that a qualifying request include at least one identifier at the subscription level, and at least one at the device level, the Commission took steps to ensure that complete disabling can occur and limit instances of potential abuse.

Section 20.23(c)(3), (3)(iii)-(iv), (4)(i)-(ii), (v):

With the disabling timeframe the Commission adopted, it sought to balance public safety interests and wireless provider concerns. The Commission found that a two-day period is sufficient for a wireless provider to analyze the request and take reasonable and practical steps to prevent an identified contraband wireless device from being used on its own network or another wireless provider's network. A wireless provider may choose to contact the customer of record through any available means (e.g., text, phone, e-mail). The Commission

**Section 20.23(b)(1), (3)-(5), (7); (c)(1)-(2), (3), (3)(iii)-(iv), (4)(i)-(ii), (v); and (d),
Contraband wireless devices in correctional facilities**

found, on balance, that it was appropriate to give a wireless provider the discretion to decide whether to contact a customer given the steps taken in the interest of public safety. With regard to DCFO notification, the Commission established the timeframe to ensure that a wireless provider responds to a DCFO within a reasonable timeframe—while giving the provider an opportunity to determine if there is an error—and to give the DCFO time to respond quickly if the request has been rejected.

With the reversal process that the Commission adopted, it sought to balance public safety interests by giving wireless providers the ability to reverse the disabling action and the choice to involve the DCFO. A wireless provider is in the best position to subsequently reverse a disabling action if it determines that the device was identified erroneously as contraband. The Commission gave the wireless provider the option, to reduce the burden on both the wireless provider and the DCFO, to involve the DCFO in the review process when determining if the device was erroneously identified as contraband. Regarding the DCFO's notification of reversals to the Contraband Ombudsman, the Commission sought to ensure that there was a way of reviewing the effectiveness of each CIS system and the DCFO process that safeguards the integrity and accuracy of the disabling process.

Section 20.23(d):

The Commission found that a limited notification requirement is necessary to deploy and use MAS effectively and ensure its ongoing effectiveness. The Commission found that the limited burden imposed by this requirement is outweighed by its significant public interest benefits. Regarding the rule adopted requiring advance notice only for limited categories of major network changes occurring within 15 miles of a correctional facility with an authorized MAS, the Commission found that a notification requirement is appropriate for such changes that could impact MAS operations nationwide and involve significant technical changes that occur only a limited number of times per year. The minimum advance notice is required to give MAS operators sufficient time to make necessary adjustments to maintain the effectiveness of their systems. The Commission found that requiring notice 90 days in advance of making network changes would neither condense nor significantly alter the timeframe in which wireless providers plan and deploy new technology. The Commission found that, on balance, the benefits to MAS operators in adopting a limited, standardized notification policy for major network changes outweigh the minimal costs imposed on CMRS licensees. To ensure that issues regarding notification to solutions providers of more frequent, localized wireless provider network changes are appropriately considered, the Commission found it in the public interest to require CMRS licensees and MAS operators to negotiate in good faith to reach an agreement for notification for those types of network adjustments not covered by the notice requirement. The Commission noted that the record supports the need for a notification exception to ensure that wireless providers are not restricted in their ability to respond quickly during times of public or national emergency and found it appropriate to require CMRS licensees to provide notice of these technical changes immediately after the exigency to ensure

**Section 20.23(b)(1), (3)-(5), (7); (c)(1)-(2), (3), (3)(iii)-(iv), (4)(i)-(ii), (v); and (d),
Contraband wireless devices in correctional facilities**

that operators continue to be notified of network changes that could impact the effectiveness of the MAS to make necessary adjustments.

These information collections do not affect individuals or households; thus, there are no impacts under the Privacy Act.

The Commission has authority for this information collection pursuant to Sections 1, 2, 4(i), 4(j), 301, 302, 303, 307, 308, 309, 310, and 332 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 152, 154(i), 154(j), 301, 302a, 303, 307, 308, 309, 310, and 332.

2. Indicate how, by whom and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information received from the current collection.

The collections in section 20.23(b)(1) regarding the application to obtain new CIS certification currently are and will be used by the Bureau to determine whether to certify a system and ensure that the systems are designed to support operational readiness and minimize the risk of disabling a non-contraband device, and ensure, to the greatest extent possible, that only devices that are in fact contraband will be identified for disabling. Bureau certification also enables targeted industry review of solutions by allowing interested stakeholders to provide feedback on the application for certification, including the proposed test plan.

The collections in section 20.23(b)(3) include the requirement that the CIS operator must file with the Bureau a self-certification that complies with paragraph (b)(3)(ii) of section 20.23, confirming that the testing at that specific correctional facility is complete and successful, and the CIS operator must serve notice of the testing on all relevant wireless providers prior to testing and provide such wireless providers a reasonable opportunity to participate in the tests. Self-certification is and will be helpful to the Bureau to ensure that qualifying requests identify contraband wireless devices accurately and in accordance with legal requirements. In addition to being used by the Bureau, the self-certification is and will be relied upon by the DCFO in conjunction with qualifying requests for disabling at a particular correctional facility. The serving of notice to the wireless providers currently does and will continue to give them awareness and an opportunity to participate in the process.

Section 20.23(b)(4) requires that wireless providers objecting to the certification filing submit objections to the Bureau within five business days and serve the DCFO and the CIS operator, which allows all stakeholders to participate in the process and raise objections. Section 20.23(b)(5) requires that CIS operators retest and recertify their systems at least every three years and comply with the same requirements as for initial self-certification. This requirement currently does and will continue to enable the Bureau to ensure the ongoing accuracy and reliability of a given CIS at a particular facility. Section 20.23(b)(7) requires that a CIS operator retain records for at least five years and provide them upon request to the Bureau, which will support the Bureau's efforts to identify issues with CIS operations, resolve

**Section 20.23(b)(1), (3)-(5), (7); (c)(1)-(2), (3), (3)(iii)-(iv), (4)(i)-(ii), (v); and (d),
Contraband wireless devices in correctional facilities**

interference issues, and resolve complaints related to misidentification of contraband devices. The requirements in these rules are all renewals of previously approved collections.

The collections in section 20.23(c)(1)-(2) include the requirement that individuals that seek to be recognized on the Commission's DCFO list must send a letter to the Contraband Ombudsperson in order for the Commission to approve that person for the qualified DCFO list and provide certainty to wireless providers that disabling requests are made by duly authorized individuals. Qualifying requests that include the required information currently are and will continue to be used by wireless carriers to prevent use of contraband devices on their network and on other wireless provider networks.

The collections in section 20.23(c)(3)(iii)-(iv) provide that, upon receiving a disabling request from a DCFO, the wireless provider must verify the request, may reject the request and must notify the DCFO whether it is accepting or rejecting the request. This process currently does and will continue to ensure that a wireless provider responds to a DCFO within a reasonable timeframe—while giving the provider an opportunity to determine if there is an error—and to give the DCFO time to respond quickly if the request has been rejected. The wireless provider may contact the customer of record to notify them of the disabling and involve them in the process.

The collections in section 20.23(c)(4) provide that a wireless provider may reverse a disabled device where it determines that the device was erroneously identified as contraband, and the wireless provider must notify the DCFO of the reversal. The wireless provider may choose to involve the DCFO in the review and reversal process. The DCFO must also provide notice to the Contraband Ombudsperson of the number of erroneously disabled devices. This process currently does and will continue to ensure the integrity of the contraband device disabling process by giving the wireless provider the opportunity to reverse a disabled device—with the ability to extend review to the DCFO—and by creating safeguards to make sure that the process is efficient and reliable.

The collections in section 20.23(d) regarding notification from CMRS licensees to MAS operators of technical changes to their network are required so that MAS operators are given sufficient time to make necessary adjustments to maintain the effectiveness of their interdiction systems. In order to ensure that issues regarding notification to solutions providers of more frequent, localized wireless provider network changes are appropriately considered, CMRS licensees and MAS operators must negotiate in good faith to reach an agreement for notification for those types of network adjustments not covered by the notice requirement. CMRS licensees must provide notice of technical changes associated with an emergency immediately after the exigency to ensure that MAS operators continue to be notified of network changes that could impact MAS effectiveness.

3. Describe whether, and to what extent, the collection of information involves the use of automated, electronic, mechanical, or other technological collection techniques

**Section 20.23(b)(1), (3)-(5), (7); (c)(1)-(2), (3), (3)(iii)-(iv), (4)(i)-(ii), (v); and (d),
Contraband wireless devices in correctional facilities**

or other forms of information technology, e.g., permitting electronic submission of responses, and the basis for the decision for adopting this means of collection. Also describe any consideration of using information technology to reduce burden.

For the collections described herein that involve Commission submissions or filings (CIS certification applications, self-certifications, periodic re-certifications, DCFO letter to the Contraband Ombudsperson), the Commission did not specify a required method of filing. The Commission also did not specify a required method of submission regarding the CIS operators serving notice of testing on all relevant wireless providers, objections filed with the Bureau by wireless providers, the service of objections, customer outreach regarding disabling, notification between the DCFO and the wireless providers of the disabling decisions and reversals, notification to the Contraband Ombudsperson of erroneous disabling, or the provision of records to the Bureau upon request. The Commission, however, directed the Bureau to issue a public notice, which was released in December 2021 (*CIS Guidance Public Notice*, GN Docket No. 13-111, DA 21-1572), describing the submission requirements. In the *CIS Guidance Public Notice*, the Bureau stated that most such filings will be submitted to the Bureau via the Commission's Electronic Comment Filing System (ECFS) and/or served electronically, as applicable. The Commission did specify that CIS operators must serve the self-certification via electronic means on all relevant wireless providers.

Regarding the transmission of a qualifying disabling request from a DCFO to a wireless provider, the Commission specified that the DCFO must transmit a qualifying request to a CMRS licensee using a secure communication means that will provide certainty regarding the identity of both the sending and receiving parties and that a CMRS licensee must adopt a method, or use an existing method, for receiving secured and verified qualifying requests. The Commission did not specify how a request is rejected or how the wireless provider must notify the DCFO that the request has been granted or rejected, but instead left it to the DCFO(s) and the wireless provider(s) to determine the best means of informing one another as long as such a request or notification is also be transmitted using the same secure communication means.

Regarding the requirement that wireless providers give notice to MAS operators of certain technical changes, the Commission did not specify a method of notification. We anticipate that notification will continue to be given via electronic means.

- 4. Describe efforts to identify duplication. Show specifically why any similar information already available cannot be used or modified for use for the purposes described in item 2 above.**

The Second Report and Order's information collections are specific to the Commission's process for implementing qualifying requests for disabling of contraband

**Section 20.23(b)(1), (3)-(5), (7); (c)(1)-(2), (3), (3)(iii)-(iv), (4)(i)-(ii), (v); and (d),
Contraband wireless devices in correctional facilities**

wireless devices in correctional facilities. Therefore, there is no similar data available and this is not a duplication effort by the Commission or any other agency.

5. If the collection of information impacts small businesses or other small entities, describe any methods used to minimize burden.

The information collections resulting from the Second Report and Order applies to all entities in the same manner. The Commission believes that applying the same rules equally to all entities in this context promotes fairness and does not believe the costs or burdens will unduly burden small entities. The Commission has taken steps to minimize the economic impact on small and other impacted entities with the rules adopted by providing flexibility, minimum requirements, and permitting and encouraging negotiations and collaboration between the parties subject to the requirements rather than adopting additional rules.

In the Second Report and Order, the Commission considered various options and minimized burdens on small entities. To minimize burdens, the Commission adopted processes and procedures where possible to allow direct interaction between the DCFOs and the wireless providers and avoided interjecting the Commission and additional regulations into the process. The Commission sought to provide small and other entities flexible options such as giving DCFOs and wireless providers the flexibility to structure the format of the qualifying requests in a way that meets the unique needs of the parties rather than adopting a standardized form. The Commission also adopted minimum requirements for information to be included in a qualifying request to disable a contraband device and allowed for self-certification to meet the certification requirements.

6. Describe the consequence to Federal program or policy activities if the collection is not conducted or is conducted less frequently, as well as any technical or legal obstacles to reducing burden.

Congress has long focused on the need to address use of contraband devices to engage in activity that endangers prison employees, other incarcerated people, and members of the public. In an Explanatory Statement to the 2021 Consolidated Appropriations Act, Congress urged the Commission to adopt a rules-based approach to requiring immediate disabling of contraband devices by a wireless carrier upon proper identification of the device. The collections in the Second Report and Order are necessary to address Congressional concerns and implement the adopted framework requiring the disabling of contraband wireless devices detected in correctional facilities upon satisfaction of certain criteria. The Commission also adopted rules requiring advance notice of certain wireless provider network changes to promote and maintain contraband interdiction system effectiveness.

**Section 20.23(b)(1), (3)-(5), (7); (c)(1)-(2), (3), (3)(iii)-(iv), (4)(i)-(ii), (v); and (d),
Contraband wireless devices in correctional facilities**

More specifically, regarding CIS certification, the technical requirements currently do and will continue to help ensure that the systems for detecting contraband wireless devices are designed to support operational readiness and minimize the risk of disabling a non-contraband device. Requiring a description of the proposed test plan will ultimately promote efficient CIS deployment and will facilitate Commission review of the systems for operational readiness prior to actual deployment.

The self-certification requirements currently do and will continue to aid in ensuring that qualifying requests identify contraband wireless devices accurately and in accordance with relevant legal authorities. Prior to initiating testing at a correctional facility site, the CIS operator must serve notice of the testing on all relevant wireless providers and provide each such provider a reasonable opportunity to participate in the tests. A CIS operator must serve via electronic means a copy of the self-certification on all relevant wireless providers, and it must subsequently submit the self-certification to the Bureau. The Commission found it appropriate to afford wireless providers that receive a self-certification five business days from the certification filing date to submit objections to the Bureau, and any such objections must be served on the DCFO and the CIS operator. 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. This process and time frame allow the wireless providers to be involved in the process while acknowledging the urgency of the need to disable contraband devices. 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. The Commission found that requiring CIS operators to maintain records will support robust efforts to identify issues with CIS operations, resolve interference issues, and resolve complaints related to misidentification of contraband devices.

With regard to qualifying requests, the requirements for DCFOs eligible to send qualifying requests to wireless providers are necessary to ensure an efficient process that safeguards the integrity and accuracy of the disabling process. The disabling timeframe adopted by the Commission seeks to balance public safety interests and wireless provider concerns. First, the two-day period for responding to qualifying requests strikes an appropriate balance between the significant public interest benefits of ensuring that contraband wireless devices, given the known dangers associated with their use, are rapidly disabled, and ensuring that wireless providers can perform the steps necessary to disable the device at both the subscriber and device levels. Second, the Commission found that a two-day period is sufficient for a wireless provider to take reasonable and practical steps to prevent an identified contraband wireless device from being used on its own network or another wireless provider's network.

Within two business days of receiving a qualifying request, a wireless provider must notify a DCFO whether the request has been granted. The Commission established this timeframe to ensure that a wireless provider responds to a DCFO within a reasonable

**Section 20.23(b)(1), (3)-(5), (7); (c)(1)-(2), (3), (3)(iii)-(iv), (4)(i)-(ii), (v); and (d),
Contraband wireless devices in correctional facilities**

timeframe—while giving the provider an opportunity to determine if there is an error—and to give the DCFO time to respond quickly if the request has been rejected.

With regard to the reversals of disabled devices and the notifications to the DCFO and Contraband Ombudsperson, the notifications are required to ensure the integrity of the contraband device disabling process by giving the wireless provider the opportunity to reverse a disabled device—with the ability to extend review to the DCFO—and by creating safeguards to make sure that the process is efficient and reliable.

With regard to notification to MAS providers of wireless provide system technical changes, the notification is required in order to ensure the ongoing effectiveness of MAS systems. The Commission found it in the public interest to require CMRS licensees leasing spectrum for operation of MAS in a correctional facility to provide 90 days' advance notice to lessees of certain technical changes, which balances the objectives of providing MAS operators sufficient advance notice of significant changes likely to impact the MAS to make technical adjustments, while not unduly burdening wireless providers.

- 7. Explain any special circumstances that cause an information collection to be conducted in a manner: requiring respondents to report information to the agency more often than quarterly; requiring respondents to prepare a written response to a collection of information in fewer than 30 days after receipt of it; requiring respondents to submit more than an original and two copies of any document; requiring respondents to submit proprietary trade secrets, or other confidential information unless the agency can demonstrate that it has instituted procedures to protect the information's confidentiality to the extent permitted by law.**

This renewal for collections of information is consistent with the guidelines in 5 CFR § 1320.

- 8. If applicable, provide a copy and identify the date and page number of publication in the Federal Register of the agency's notice, required by 5 CFR 1320.8(d), soliciting comments on the information prior to submission to OMB.**

Describe efforts to consult with persons outside the agency to obtain their views on the availability of data, frequency of collection, the clarity of instructions and recordkeeping, disclosure, or reporting format (if any), and on the data elements to be recorded, disclosed, or reported.

The Commission published a 60-day notice for the Second Report and Order requirements that appeared in the Federal Register on October 25, 2024, (89 FR 85208) seeking comment from the public on the information collection requirements contained in this

**Section 20.23(b)(1), (3)-(5), (7); (c)(1)-(2), (3), (3)(iii)-(iv), (4)(i)-(ii), (v); and (d),
Contraband wireless devices in correctional facilities**

collection. No comments were received on the Paperwork Reduction Act (PRA) as a result of the notice.

9. Explain any decision to provide any payment or gift to respondents, other than remuneration of contractors or grantees.

No gift or payments will be given to respondents for this collection.

10. Describe any assurance of confidentiality provided to respondents and the basis for the assurance in statute, regulation or agency policy.

With regard to the CIS certification process, respondents may request that materials or information submitted to the Commission be withheld from public inspection under 47 CFR § 0.459 of the FCC. The Commission will evaluate such requests on a case-by-case basis. As directed by the Commission in the Second Report and Order, the Bureau outlined a process for review of CIS applications by interested stakeholders in the *CIS Guidance Public Notice*, and established procedures that maintain the confidentiality, to the extent appropriate, of certain categories of sensitive information via Protective Order, GN Docket No. 13-111, DA 23-223.

11. Provide additional justification for any questions of a sensitive nature.

No sensitive information is required for this collection.

12. Provide estimates of the hour burden of the collection of information. The statement should: indicate the number of respondents, frequency of response, annual hour burden, and an explanation of how the burden was estimated. If the hour burden on respondents is expected to vary widely because of differences in activity, size, or complexity, show the range of estimated hour burden, and explain the reasons for the variance.

Section 20.23(b)(1), (3)-(5), (7)

A CIS operator seeking to obtain CIS certification authorizing the submission of qualifying disabling requests must file an application with the Bureau for review and approval. The preparation and filing of the specific legal and technical CIS certification requirements is a not a new burden for the CIS operator.

The CIS operator seeking to use the CIS to submit qualifying requests for disabling must test a certified CIS at each location where it intends to operate and serve notice of the testing on all relevant wireless providers prior to testing so that such wireless providers have a reasonable opportunity to participate in the tests. Notice to the wireless providers is

**Section 20.23(b)(1), (3)-(5), (7); (c)(1)-(2), (3), (3)(iii)-(iv), (4)(i)-(ii), (v); and (d),
Contraband wireless devices in correctional facilities**

accomplished electronically and the response, if any, from the wireless provider to the CIS operator will also be given electronically.

Following the site-based testing, the CIS operator must file a self-certification with the Bureau that confirms that the testing at the specific correctional facility is complete and successful. The preparation and filing of the self-certification is not a new burden for the CIS operator.

Within five days from the certification filing date, wireless providers may file an objection with the Bureau, with a copy served on the DCFO and CIS operator. The preparation, filing, and service of the certification objection is not a new burden for the wireless providers. While we have yet to receive any such filings, we anticipate that most such filings will be accomplished electronically.

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. The CIS operator must comply with the same rules and filing instructions that apply to the initial self-certification. The recertification process is not a new burden on the CIS operator and the wireless provider, where the wireless provider must be given notice of the testing, the opportunity to participate in that testing, and the opportunity to submit a CIS certification response. These filings will be submitted to the Bureau via ECFS or served electronically.

To ensure the integrity and proper operation of CISs, a CIS operator must retain records of all information supporting each request for disabling and the basis for disabling each device, including copies of all documents submitted in the qualifying request, for at least five years following the date of submission of the relevant disabling request. CIS operators of systems that have been tested and approved for use in qualifying requests must make available all records upon request from the Bureau. The maintenance of the records and submitting to the Bureau upon request is not a new burden for CIS operators.

Commission records reflect that there are 8 CIS operators that have filed CIS certification applications over the past three year collection period. We anticipate that a total of 2 CIS providers will submit CIS certification applications per year pursuant to this rule for the 3-year certification period.

In addition, Commission records reflect that there are on average 3 active wireless providers that operate on the frequencies covering a correctional facility at which a CIS operator seeks to detect contraband use. Thus, the Commission anticipates that a CIS operator for each correctional facility will have to notify and give the opportunity to participate in the testing at each facility to, on average, 3 wireless providers.

**Section 20.23(b)(1), (3)-(5), (7); (c)(1)-(2), (3), (3)(iii)-(iv), (4)(i)-(ii), (v); and (d),
Contraband wireless devices in correctional facilities**

Commission records reflect that there are approximately 318 correctional facilities nationwide at which a CIS operator has an active lease authorizing CIS deployment.¹ Commission records also reflect that we received 7 self-certifications over the last three year period. Based upon the number of self-certifications that the Commission has received over the last 3-year certification period, we anticipate that, on average, CIS operators will submit 60 self-certifications during the next 3-year certification period, resulting in an average of approximately 20 self-certifications submissions annually.

The Commission estimates that each CIS application will require the CIS operator to spend 20 hours collecting the information to be submitted with the CIS application and submitting the application to the Bureau. The Commission estimates that self-certification will require the CIS operator to spend 10 hours analyzing the information to be submitted, researching the state law relevant to contraband device use in correctional facilities, notifying relevant wireless providers, and submitting the self-certification to the Bureau.² The Commission also estimates that CIS operators will spend 2 hours on records maintenance. Thus, the estimated annual burden hours for the CIS operators = [20 (hours related to CIS applications) x 2 (# of new CIS operators) = 40/3 = 13 hours annually] + [2 hours x 10 (# of current and new CIS operators) = 20 hours annually for records maintenance] + [20 (# of correctional facilities where self-certification is sought annually) x 10 (hours related to self-certification preparation and related task = 200 hours annually)] + [3 (# of correctional facilities where recertification will be sought annually) x 10 (hours related to self-certification preparation and related task = 30 hours annually)] = 13 + 20 + 200 + 30 = 263 total hours annually.

Total Number of Respondents: 14 CIS operators

Total Annual Responses: 2 CIS certification applications + 20 CIS self-certifications + 3 CIS recertifications = 25 responses

Total Annual Hourly Burden: 263 hours

In-House Cost – CIS Operator: The Commission estimates that the CIS operators will utilize in-house resources for these applications. The Commission estimates that the hourly wage of a full-time in-house regulatory staff employee of a CIS operator is \$70/hour. Therefore, the estimated in-house cost is as follows: 263 hours x \$70/hour = \$18,410.

The Commission estimates that wireless providers will be required to spend 2 hours reviewing and responding, if necessary, to each CIS certification application. The Commission estimates that a wireless provider will also spend 2 hours researching, analyzing test data, and

¹ We note that typically departments of correction contract with no more than one CIS operator per correctional facility.

² CIS operators will be subject to recertification after the initial three-year period and therefore the burden estimates are relevant for the subsequent three-year periods.

**Section 20.23(b)(1), (3)-(5), (7); (c)(1)-(2), (3), (3)(iii)-(iv), (4)(i)-(ii), (v); and (d),
Contraband wireless devices in correctional facilities**

drafting any objection to the self-certifications, filing, and serving the response on the Bureau, the DCFO, and CIS operator. This estimate is based on the level of interest and importance of CIS certifications to the wireless providers and the fact that the wireless provider has 5 days in which to respond to the self-certification. Thus, the estimated annual burden hours for a wireless provider = [2 hours x 2 (# of CIS certification applications) = 4 hours annually] + [2 hours x 20 (# of CIS self-certifications annually) = 40 hours] + [2 hours x 3 (# of correctional facilities where recertification will be sought annually) = 6 hours] = 4 + 40 + 6 = 50 total hours annually.

Total Number of Respondents:³ 3 wireless providers

Total Annual Responses: 6 wireless responses to CIS certification applications + 20 wireless responses to self-certifications per wireless provider + 6 wireless responses to recertifications per wireless provider = 32 responses

Total Annual Hourly Burden: 50 hours

In-House Cost – Wireless Provider: The Commission estimates that the wireless provider will utilize in-house resources for work related to objecting to the CIS certification applications and self-certifications. The Commission estimates that the hourly wage of a full-time in-house regulatory staff employee of a wireless provider is \$70/hour. Therefore, the in-house cost is as follows: 50 hours x \$70/hour = \$3,500.

Section 20.23(c)(1)-(2)

The rules require that a DCFO must request authorization to transmit qualifying requests from the Commission's Contraband Ombudsperson. The list of qualified DCFOs will be maintained on the Commission's website. Requiring the DCFO to seek authorization from the Commission's Contraband Ombudsperson is not a new burden.

A DCFO must submit a qualifying request to a CMRS licensee asking the CMRS licensee to disable a contraband wireless device that has been detected in a correctional facility by a CIS that has been certified pursuant to the Commission's rules. The DCFO must transmit a qualifying request to a CMRS licensee using a secure communication means that will provide certainty regarding the identity of both the sending and receiving parties. A CMRS licensee must adopt a method, or use an existing method, for receiving secured and verified qualifying requests. The burden to submit a qualifying request using a secure means to a CMRS licensee is not a new burden for DCFOs. In addition, the burden to securely receive and verify a qualifying request from a DCFO is not a new burden for a CMRS licensee. But it should be noted that we expect that the burden on CMRS licensees will be alleviated since some licensees

³ Although we estimate a total number of 3 wireless providers here, this number is not restricted by rule to 3 and could be 10 or more in the future. Therefore, we are seeking OMB clearance of this information collection.

**Section 20.23(b)(1), (3)-(5), (7); (c)(1)-(2), (3), (3)(iii)-(iv), (4)(i)-(ii), (v); and (d),
Contraband wireless devices in correctional facilities**

already have existing secure portals to receive court-ordered termination requests. We anticipate that the qualifying request will continue to be sent electronically.

Commission records reflect that there are approximately 318 correctional facilities nationwide at which a CIS operator has an active lease authorizing CIS deployment.⁴ Commission records also reflect that we received 7 self-certifications over the last three year period. Based upon the number of self-certifications that the Commission has received over the last 3-year certification period, we anticipate that, on average, CIS operators will submit 60 self-certifications during the next 3-year certification period, resulting in an average of approximately 20 self-certifications submissions annually.

To date, the Commission has received 7 DCFO authorization requests. These requests cover 7 states and each request includes multiple correctional facilities within that state. On average, each state has requested authorization for 3 individuals to be DCFOs within its DCFO authorization request. Thus, the Commission anticipates that it will receive an additional 21 DCFOs (50 states - 7 states with current DCFOs) authorization submissions to send qualifying requests pursuant to this rule for the 3-year certification period, resulting in an average of 7 authorization submissions annually.

In addition, we anticipate that each DCFO will submit, on average, 52 qualifying requests (approximately 1 request per week) annually.

The Commission estimates that each authorization request to be added to the DCFO list will require the DCFO to spend 1 hour preparing and sending the authorization request to the Contraband Ombudsperson. The Commission also estimates that a DCFO will spend approximately 10 hours analyzing, preparing, drafting, certifying, and sending each qualifying request to CMRS licensees. Thus, the estimated annual burden hours for DCFOs = [7 authorization requests x 1 hour = 7 hours annually (for DCFO authorizations)] + [10 hours per qualifying request x 52 qualifying requests = 520 hours annually] x 14 (# of DCFOs submitting qualifying requests annually) = 7,378 total hours annually.

Total Number of Respondents: 14 DCFOs

Total Annual Responses: 7 DCFO authorization requests + 52 x 14 DCFOs submitting qualifying requests = 735 responses

Total Annual Hourly Burden: 7,278 hours

In-House Cost – DCFO: The Commission estimates that the DCFO will utilize in-house resources for the request to be on the DCFO list and the analyzing, preparing, drafting, certifying, and sending of the qualifying requests. The Commission estimates that the hourly

⁴ We note that typically departments of correction contract with no more than one CIS operator per correctional facility.

**Section 20.23(b)(1), (3)-(5), (7); (c)(1)-(2), (3), (3)(iii)-(iv), (4)(i)-(ii), (v); and (d),
Contraband wireless devices in correctional facilities**

wage of a DCFO is \$60/hour. Therefore, the in-house cost is as follows: 7,278 hours x \$60/hour = \$436,680.

Section 20.23(c)(3), (c)(3)(iii)-(iv)

Once a CMRS licensee receives the qualifying request from a DCFO, the licensee must verify that the request contains the required information for a qualifying request as specified in Commission rules. A licensee may reject a qualifying request within two business days of receipt of a qualifying request if it does not include the information required for a qualifying request or, with respect to a relevant device, the request contains an error in the device-identifying information preventing the licensee from being able to disable the device. A licensee may immediately disable a contraband wireless device without any customer outreach, or a licensee may contact the customer of record through any available means to notify them that the device will be disabled. Within two business days of receiving a qualifying request from a DCFO, a licensee must inform the DCFO whether the request has been granted or rejected. The receipt of the qualifying request, rejecting or granting that request, notifying a consumer of, and notifying the DCFO of the disabling of the device is a burden for a CMRS licensee. However, several wireless providers already have internal procedures for disabling contraband wireless devices which could be modified to accommodate this disabling process. Thus, reducing some of the burden on wireless providers. We anticipate that the CMRS licensee will make all communications electronically.

Commission records reflect that there are, on average, 3 CMRS licensees that operate on frequencies covering a correctional facility on which a CIS operator seeks to detect contraband use. The Commission anticipates that in each year of the 3-year certification period, there will continue to be, on average, 3 CMRS licensees with spectrum covering each correctional facility.

Commission records reflect that there are approximately 318 correctional facilities nationwide at which a CIS operator has an active lease authorizing CIS deployment.⁵ Commission records also reflect that we received 7 self-certifications over the last three year period. Based upon the number of self-certifications that the Commission has received over the last 3-year certification period, we anticipate that, on average, CIS operators will submit 60 self-certifications during the next 3-year certification period, resulting in an average of approximately 20 self-certifications submissions annually.

To date, the Commission has received 7 DCFO authorization requests. These requests cover 7 states and each request includes multiple correctional facilities within that state. On average, each state has requested authorization for 3 individuals to be DCFOs within its DCFO authorization request. Thus, the Commission anticipates that it will receive an additional 21

⁵ We note that typically departments of correction contract with no more than one CIS operator per correctional facility.

**Section 20.23(b)(1), (3)-(5), (7); (c)(1)-(2), (3), (3)(iii)-(iv), (4)(i)-(ii), (v); and (d),
Contraband wireless devices in correctional facilities**

DCFOs (50 states - 7 states with current DCFOs) authorization submissions to send qualifying requests pursuant to this rule for the 3-year certification period, resulting in an average of 7 authorization submissions annually.

In addition, we anticipate that each DCFO will submit, on average, 52 qualifying requests (approximately 1 request per week) annually. Thus, we anticipate that, on average, a CMRS licensee will receive 728 qualifying requests annually (14 DCFOs submitting qualifying requests x 52).

The Commission estimates that each qualifying request will require the CMRS licensee to spend 10 hours reviewing, analyzing, verifying, making a determination on, contacting customers, and preparing and sending the notification of the decision to the DCFO. Thus, the estimated annual burden hours for the CMRS licensee = 10 hours x 728 = 7,280 total hours annually.

Total Number of Respondents⁶: 3 CMRS licensees

Total Annual Responses: 728 qualifying requests per CMRS licensee

Total Annual Hourly Burden: 7,280 hours per CMRS licensee

In-House Cost – CMRS Licensee: The Commission estimates that the CMRS licensee will utilize in-house resources for handling the qualifying requests. The Commission estimates that the hourly wage of a full-time in-house regulatory staff employee of a CMRS licensee is \$70/hour. Therefore, the in-house cost is as follows: 7,280 hours x \$70/hour = \$509,600.

Section 20.23(c)(4)(i)-(ii), (v)

A CMRS 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 and may request that the DCFO review and confirm the information provided in a qualifying request pursuant to which the device was previously disabled. Upon receipt of a request from a wireless provider, the DCFO should review the qualifying request and determine whether the device in question was erroneously identified and either confirm the validity of the identifying information contained in the qualifying request or acknowledge the error and direct the carrier to restore service to the device. The DCFO 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.

⁶ Although we estimate a total number of 3 wireless providers here, this number is not restricted by rule to 3 and could be 10 or more in the future. Therefore, we are seeking OMB clearance of this information collection.

**Section 20.23(b)(1), (3)-(5), (7); (c)(1)-(2), (3), (3)(iii)-(iv), (4)(i)-(ii), (v); and (d),
Contraband wireless devices in correctional facilities**

Commission records reflect that there are, on average, 3 CMRS licensees that operate on frequencies covering a correctional facility on which a CIS operator seeks to detect contraband use. The Commission anticipates that in each year of the 3-year certification period, there will continue to be, on average, 3 CMRS licensees with spectrum covering each correctional facility.

Commission records reflect that there are approximately 318 correctional facilities nationwide at which a CIS operator has an active lease authorizing CIS deployment. Commission records also reflect that we received 7 self-certifications over the last three year period. Based upon the number of self-certifications that the Commission has received over the last 3-year certification period, we anticipate that, on average, CIS operators will submit 60 self-certifications during the next 3-year certification period, resulting in an average of approximately 20 self-certifications submissions annually.

To date, the Commission has received 7 DCFO authorization requests. These requests cover 7 states and each request includes multiple correctional facilities within that state. On average, each state has requested authorization for 3 individuals to be DCFOs within its DCFO authorization request. Thus, the Commission anticipates that it will receive an additional 21 DCFOs (50 states - 7 states with current DCFOs) authorization submissions to send qualifying requests pursuant to this rule for the 3-year certification period, resulting in an average of 7 authorization submissions annually.

In addition, we anticipate that each DCFO will submit, on average, 52 qualifying requests (approximately 1 request per week) annually. Thus, we anticipate that, on average, CMRS licensees will receive 728 qualifying requests annually (14 DCFOs submitting qualifying requests annually x 52). We anticipate that 2 out of the 52 qualifying requests submitted by each DCFO will result in a reversal. Therefore, given that we anticipate 728 qualifying requests annually, we anticipate that 28 reversals will result annually.

The Commission estimates that each reversal will require the CMRS licensee to spend 10 hours gathering and providing information to the DCFO to trigger the DCFO's involvement, reviewing, analyzing, verifying, and making a determination on the decision to reverse, and preparing and sending the notification of the decision to the DCFO. Thus, the estimated annual burden hours on each CMRS licensee = 10 hours x 28 reversals annually = 280 hours annually.

Total Number of Respondents:⁷ 3 CMRS licensees
Total Annual Responses from CMRS licensees: 28 reversals
Total Annual Hourly Burden: 280 hours per CMRS licensee

⁷ Although we estimate a total number of 3 wireless providers here, this number is not restricted by rule to 3 and could be 10 or more in the future. Therefore, we are seeking OMB clearance of this information collection.

**Section 20.23(b)(1), (3)-(5), (7); (c)(1)-(2), (3), (3)(iii)-(iv), (4)(i)-(ii), (v); and (d),
Contraband wireless devices in correctional facilities**

In-House Cost – CMRS Licensee: The Commission estimates that the CMRS licensee will utilize in-house resources for this process. The Commission estimates that the hourly wage of a full-time in-house regulatory staff employee of a CMRS licensee is \$70/hour. Therefore, the in-house cost is as follows: 280 hours x \$70/hour = \$19,600.

The Commission estimates that each reversal will require the DCFO, when its involvement is triggered by the CMRS licensee, to spend 10 hours reviewing, analyzing, verifying, making a determination on, and preparing and sending the notification of the decision to the CMRS licensee. The Commission also estimates that a DCFO will spend 2 hours preparing and sending the quarterly reversal notifications to the Commission's Contraband Ombudsperson, resulting in 8 hours annually. Thus, the estimated annual hour burden is 10 hours x 28 reversals annually = 280, plus 8 hours = 288 hours annually.

Total Number of Respondents: 14 DCFOs
Total Annual Responses: 28 reversals
Total Annual Hourly Burden: 288 hours

In-House Cost – DCFO: The Commission estimates that the DCFO will utilize in-house resources for the qualifying requests. The Commission estimates that the hourly wage of a DCFO is \$70/hour. Therefore, the in-house cost is as follows: 288 hours x \$70/hour = \$20,160.

Section 20.23(d)

The MAS operator notification rules require that CMRS licensees leasing spectrum to MAS operators must provide 90 days' advance notice to MAS operators of the specific network changes occurring within 15 miles of the correctional facility, unless parties modify notification arrangements through mutual agreement. The Commission's rules also require CMRS licensee lessors and MAS operator lessees to negotiate in good faith to reach an agreement for notification for other types of network adjustments not covered by the notice requirement set forth in paragraph (d)(1) of this section and for the parties' treatment of confidential information contained in notifications required pursuant to this rule section and/or negotiated between the parties. Regarding notifications required due to emergency and disaster preparedness, CMRS licensees must provide notice of these technical changes immediately after the exigency.

Commission records reflect that there are, on average, 3 CMRS licensees leasing spectrum to MAS operators. The Commission anticipates that in each year of the 3-year certification period, there will continue to be, on average, 3 CMRS licensees leasing spectrum to MAS operators per correctional facility.

Commission records reflect that there are 8 CIS operators that have filed CIS certification applications over the past three year collection period. We anticipate that a total of

**Section 20.23(b)(1), (3)-(5), (7); (c)(1)-(2), (3), (3)(iii)-(iv), (4)(i)-(ii), (v); and (d),
Contraband wireless devices in correctional facilities**

2 CIS providers will submit CIS certification applications per year pursuant to this rule for the 3-year certification period.

Commission records reflect that there are approximately 318 correctional facilities nationwide at which a CIS operator has an active lease authorizing CIS deployment.⁸ Commission records also reflect that we received 7 self-certifications over the last three year period. Based upon the number of self-certifications that the Commission has received over the last 3-year certification period, we anticipate that, on average, CIS operators will submit 60 self-certifications during the next 3-year certification period, resulting in an average of approximately 20 self-certifications submissions annually. Thus, we anticipate that CIS operators will seek to operate at 338 facilities over the 3-year certification period (318 existing facilities + 20 new facilities annually), resulting in, on average, 113 facilities annually.

The Commission estimates that, on average, a CMRS licensee will send 2 notifications to MAS operators annually as required by the notification rule, and because we estimate that there will be 14 CIS operators with leases at correctional facilities, a CMRS licensee will be required to send 28 notifications annually per correctional facility. Because the Commission estimates that CIS operators will operate at 113 facilities annually, a CMRS licensee will be required to send 28 notifications x 113 facilities = 3,164 notifications annually, on average.

The Commission estimates that each notification will require on average 2 hours to prepare and send to each relevant MAS operator. This estimate is based on an average of the minimal amount of time it would take a CMRS licensee to send electronic notification of the specific network change to a MAS operator. Thus, the estimated burden hours for the MAS operator notifications for each CMRS licensee = 3,164 notifications x 2 hours = 6,328 hours annually.⁹

Total Number of Respondents:¹⁰ 3 CMRS licensees

Total Annual Responses: 3,164 notifications per CMRS licensee

Total Annual Hourly Burden: 6,328 hours per CMRS licensee

In-House Cost – CMRS Licensee: The Commission estimates that the CMRS licensees will utilize in-house resources for this collection based on their knowledge of and experience with

⁸ We note that typically departments of correction contract with no more than one CIS operator per correctional facility.

⁹ We do not have a basis for estimating the number of CIS systems deployed without features of MAS that therefore do not fall within the scope of the notification requirement. Accordingly, the above conservative estimate is based on notice to all CIS operators.

¹⁰ Although we estimate a total number of 3 wireless providers here, this number is not restricted by rule to 3 and could be 10 or more in the future. Therefore, we are seeking OMB clearance of this information collection

**Section 20.23(b)(1), (3)-(5), (7); (c)(1)-(2), (3), (3)(iii)-(iv), (4)(i)-(ii), (v); and (d),
Contraband wireless devices in correctional facilities**

the MAS operators. The Commission estimates that the hourly wage of a full-time in-house regulatory staff employee of a CMRS licensee is \$70/hour. Therefore, the in-house cost is as follows: 6,328 hours x \$70/hour = \$442,960.

TOTAL NUMBER OF RESPONDENTS: 54.
TOTAL NUMBER OF ANNUAL RESPONSES: 4,740.
TOTAL BURDEN HOURS TO RESPONDENTS: 21,767 hours.
TOTAL IN-HOUSE COST TO RESPONDENTS: \$1,450,910.

13. Provide estimate for the total annual cost burden to respondents or recordkeepers resulting from the collection of information. (Do not include the cost of any hour burden shown in items 12 and 14).

There is no cost to the respondents.

14. Provide estimates of annualized costs to the Federal government. Also provide a description of the method used to estimate cost, which should include quantification of hours, operational expenses (such as equipment, overhead, printing, and support staff), any other expenses that would not have been incurred without this collection of information.

The Commission estimates that it will take an attorney at the GS-13, Step 5 earning \$64.06/hour 80 hours to: review each CIS certification application with the required supporting evidence submitted, analyze the DCFO request letters, maintain on the website a list of current DCFOs, review reversals, (review the self-certifications, review objections to the certifications, and request and review records. Thus, the estimated number of annual burden hours = 80. We estimate that the majority of the above tasks will be associated with applications filed per correctional facility, and that there will be an estimated 32 such applications annually. We therefore estimate that the total annual hour burden = 80 hours x 32 applications = 2,560 hours.

2,560 hours x \$64.06/hour = \$163,993.60

Total Annual Cost to the Federal Government is: \$163,993.60

15. Explain the reasons for any program changes or adjustments to this collection.

The Commission does not have any program changes to this collection. There are adjustments to the collection which are due to fewer respondents responding to this collection. The adjustments are as follows: -477 to the number of respondents, -11,649 to the annual number of responses and -120,801 to the annual burden hours.

16. For collections of information whose results will be published, outline plans for

**Section 20.23(b)(1), (3)-(5), (7); (c)(1)-(2), (3), (3)(iii)-(iv), (4)(i)-(ii), (v); and (d),
Contraband wireless devices in correctional facilities**

tabulation and publication.

The data will not be published.

17. If seeking approval to not display the expiration date for OMB approval of the information collection, explain the reasons that display would be inappropriate.

This information collection does not include any FCC Forms, therefore we are not seeking exemption from displaying the expiration date for OMB approval of this collection.

18. If seeking approval to not display the expiration date for OMB approval of the information collection, explain the reasons that display would be inappropriate.

There are no exceptions to the certification statement.

B. Collection of Information Employing Statistical Methods:

This information collection does not employ statistical methods.