SUPPORTING STATEMENT

A. Justification:

The Federal Communications Commission (Commission) is seeking Office of Management and Budget (OMB) approval for a new information collection. We are submitting this collection to the OMB in order to obtain the full three-year clearance.

1. *Circumstances that make these collections necessary.* On July 24, 2023, the Commission released the *Enhanced A-CAM Order* (Order), WC Docket No. 10-90 et al., FCC 23-60, which adopted a voluntary path for supporting the widespread deployment of 100/20 Mbps broadband service throughout the rural areas served by carriers currently receiving Alternative Connect America Cost Model (A-CAM) support and in areas served by rate-of-return carriers eligible to receive legacy support by the end of 2028. The Commission extended by 10 years beyond the remaining five years, for a total of 15 years, the term of support for electing carriers and set a methodology for determining support amounts for locations without 100/20 Mbps broadband service within a potential budget of no more than $1.27 billion annually, or no more than $1.33 billion annually if certain conditions are met, using an updated version of the A-CAM. By adopting this program, the Commission furthered its long-standing goals by promoting the universal availability of voice and broadband networks, while also taking measures to minimize the burden on the nation's ratepayers. The Commission also adopted requirements for the Enhanced A-CAM program to complement existing federal, state, and local funding programs, so that broadband funding can be used efficiently to maximize the deployment of high-quality broadband service across the United States.

To ensure that the Enhanced A-CAM program does not deprive rural consumers in high-cost areas of broadband service that is as secure as the service deployed pursuant to other federal funding initiatives, the Commission required Enhanced A-CAM carriers to implement operational cybersecurity and supply chain risk management plans by January 1, 2024—the start of the Enhanced A-CAM support term. Enhanced A-CAM carriers must submit such plans to the Universal Service Administrative Company (USAC) and certify they have done so, by January 2, 2024 or within 30 days of approval under the Paperwork Reduction Act, whichever is later. Failure to submit the plans and make the certification shall result in 25% of monthly support being withheld until the carrier comes into compliance. If a carrier makes a substantive modification to its cybersecurity or supply chain risk management plan, the Commission requires that the carrier submit its updated plan to USAC within 30 days of making that modification.

The Commission is seeking approval by the OMB under the Paperwork Reduction Act (PRA) of the information collection requirements contained in the new rules. The Commission plans to submit at a later date additional revisions or new collections for OMB review to address other reforms adopted in the Order.

The Commission estimates that approximately 450 carriers may accept Enhanced A-CAM offers, and thus will be subject to the cybersecurity and supply chain risk management

plan requirements. The number of carriers subject to the requirements may vary, depending on the number of carriers that accept Enhanced A-CAM offers.

The following are the new collections of information related to Enhanced A-CAM cybersecurity or supply chain risk management plans:

a. *Submission and Certification of Initial Cybersecurity and Supply Chain Risk Management Plans-47 CFR § 54.308(e)(2).*

Section 54.308(e)(2) of the Commission's rules require that by January 2, 2024, or within 30 days of approval under the Paperwork Reduction Act, whichever is later, an Enhanced A-CAM carrier must: a) certify that it has implemented operational cybersecurity and supply chain risk management plans by January 1, 2024, as required by 47 CFR § 54.308(e)(1), and the plans meet the Commission's requirements as described in 47 CFR §§ 54.308(e)(4) & (5) of the Commission's rules, and b) submit the cybersecurity and supply chain risk management plans to USAC; 47 CFR § 54.308(e)(2).

Pursuant to section 54.308(e)(4) of the Commission's rules, an Enhanced A-CAM carrier's cybersecurity risk management plans shall reflect the latest version of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, and shall reflect an established set of cybersecurity best practices, such as the standards and controls set forth in the Cybersecurity & Infrastructure Security Agency (CISA) Cybersecurity Cross-sector Performance Goals (CPGs) and Objectives or the Center for Internet Security Critical Security Controls; 47 CFR § 54.308(e)(6).

Pursuant to section 54.308(e)(5) of the Commission's rules, an Enhanced A-CAM carrier's supply chain risk management plans shall incorporate the key practices described in NISTIR 8276, Key Practices in Cyber Supply Chain Risk Management: Observations from Industry, and related supply chain risk management guidance from NIST 800-161; 47 CFR § 54.308(e)(6).

b. *Submission of Substantially Modified Cybersecurity and Supply Chain Risk Management Plans-47 CFR § 54.308(e)(6)*.

If an Enhanced A-CAM carrier makes a substantive modification to its cybersecurity and/or supply chain risk management plans, it must file its updated plan with USAC within 30 days of making the modification. A modification to a plan is substantive if at least one of the following conditions apply; 47 CFR § 54.308(e)(6):

(i) There is a change in the plan's scope, including any addition, removal, or significant alteration to the types of risks covered by the plan (e.g., expanding a plan to cover new areas such as supply chain risks to Internet of Things devices or cloud security could be a substantive change);

(ii) There is a change in the plan's risk mitigation strategies (e.g., implementing a new encryption protocol or deploying a different firewall architecture);

(iii) There is a shift in organizational structure (e.g., creating a new information technology department or hiring a Chief Information Security Officer);

(iv) There is a shift in the threat landscape prompting the organization to recognize the emergence of new threats or vulnerabilities that weren't previously accounted for in the plan;

(v) Any updates made to comply with new cybersecurity regulations, standards, or laws;

(vi) Significant changes in the supply chain, including offboarding major suppliers or vendors, or shifts in procurement strategies that may impact the security of the supply chain; or

(vii) Any large-scale technological changes, including the adoption of new systems or technologies, migrating to a new information technology infrastructure, or significantly changing the information technology architecture.

Statutory authority for this information collection is contained in 47 U.S.C. sections 154(i), 214, 218-220, 254, 303(r), and 403.

This information does not affect individuals or households; thus, there are no impacts under the Privacy Act.

2. *Use of Information.* The Commission will use the information collected to verify that Enhanced A-CAM carriers have implemented operational cybersecurity and supply chain risk management plans in accordance with the Commission's rules.

3. *Technological collection techniques.* The Commission is committed to meeting the requirements of the E-Government Act, which requires Government agencies to provide the general public the option of submitting information or transacting business electronically to the maximum extent possible. The certification and plans will be collected electronically by USAC.

4. *Efforts to identify duplication.* There will be no duplicative information collected. Each Enhanced A-CAM carrier must submit its individual certification, initial plans, and updated plans in the case of any substantial updates.

5. *Impact on small entities*. The collections of information may affect small entities as well as large entities. In conformance with the PRA, the Commission is making an effort to minimize the burden on all respondents regardless of size. The Commission affords carriers the flexibility to include standards and controls in their cybersecurity management plans that are reasonably tailored to their business needs. Moreover, carriers that already implement the NIST Framework for Improving Critical Infrastructure Cybersecurity can comply with this requirement without redoing their plan so long as they implement an established set of cybersecurity best practices. The Commission also encourages Enhanced A-CAM providers to take advantage of existing federal government resources designed to share supply chain security risk information with trusted communications providers and suppliers to facilitate the creation of cybersecurity and supply-chain risk management plans.

6. *Consequences if information is not collected.* If an Enhanced A-CAM carrier does not submit the required certification or cybersecurity and supply chain risk management plans by January 2, 2024 or within 30 days of approval under the Paperwork Reduction Act, whichever is later; the Wireline Competition Bureau will direct USAC to withhold 25 percent of the Enhanced A-CAM carrier's monthly support for failure to comply until the carrier makes the required certification and submits the required plans. Similarly, if at any point during the support term an Enhanced A-CAM carrier does not have in place operational cybersecurity and supply chain risk management plans meeting the Commission's requirements, the Wireline Competition Bureau will direct USAC to withhold 25 percent of the carrier's monthly support. Once the carrier comes into compliance, USAC will stop withholding support and the carrier will receive all of the support that has been withheld.

7. *Special circumstances.* We do not foresee any special circumstances with this information collection.

8. *Notice required by 5 CFR § 1320.8(d).* A 60-day notice was published in the *Federal Register* pursuant to 5 C.F.R. § 1320.8(d) on September 5, 2023 (88 FR 60677). We received one comment in response to this notice. *See* Comments of the NTCA—The Rural Broadband Association (NTCA) on Proposed Information Collection Requirements, OMB Control No. 3060-XXX (Enhanced A-CAM Cybersecurity and Supply Chain Risk Management Plan Requirements) (filed November 6, 2023) (NTCA Comments). The commenter is seeking to postpone the filing deadline of January 2, 2024 (or within 30 days of approval under the Paperwork Reduction Act, whichever is later) for the initial submission of cybersecurity and supply chain risk management plans. Specifically, NTCA requests that Enhanced A-CAM providers instead be required to submit their plans with their annual FCC Form 481 report due July 1, 2024. NTCA also requests that rather than submit updated plans within 30 days of a making a "substantive modification" to the plans, Enhanced A-CAM carriers be required to file substantively modified plans once per year with their FCC Form 481 reports.

   NTCA's proposals would delay the Commission's ability to ensure that Enhanced A-CAM carriers have the plans in place to offer broadband over secure networks and to monitor the carriers' continued compliance with these requirements. The Commission's adoption of the cybersecurity and supply chain risk management plan requirements "emphasize[s] the critical importance of cybersecurity and supply chain risk management in modern broadband networks . . . .", *see FCC Adopts Plan to Bring Reliable Broadband to Rural Communities*, Report and Order, 88 FR 55918 (Enhanced A-CAM Order). By adopting a deadline for the initial submission of plans as close as possible to the start of the Enhanced A-CAM carriers' support terms on January 1, 2024, the Commission will be able to identify soon after the support term starts whether any Enhanced A-CAM carriers have failed to implement the required plans and withhold support to ensure compliance. While NTCA claims that the release of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity 2.0 (CSF) may require Enhanced A-CAM carriers to submit updated plans soon after their initial submissions because NIST "expects to release an updated version of the NIST CSF in early 2024," no definitive release date has

been set. And, given the evolving environment, the risk of carriers having to update plans soon after the initial submission may be present regardless of when the Commission sets the deadline for initial submissions. Moreover, by requiring that Enhanced A-CAM carriers submit updated plans within 30 days of any substantive update, the Commission will be able to monitor throughout the support term how Enhanced A-CAM carriers are adapting to the changing cybersecurity and supply chain risk management landscape, rather than the Commission having to wait up to 18 months to see whether and what updates have been made.

The Commission has acknowledged the burdens Enhanced A-CAM carriers may face in complying with these requirements, particularly as many are small companies with limited resources. To help alleviate those burdens, the Commission explained that it took "steps to mitigate concerns that development and implementation of cybersecurity plans are expensive and time consuming," including by giving carriers the "flexibility to include standards and controls in their cybersecurity management plans that are reasonably tailored to their business needs." The Commission also directed carriers to existing federal resources to help facilitate the creation of the required plans. The burdens associated with submitting these plans by the required deadlines is outweighed by the Commission's interest in being able to timely monitor Enhanced A-CAM carriers' implementation of requirements that "will improve the cybersecurity of the nation's broadband networks and protect consumers from online risks such as fraud, theft, and ransomware that can be mitigated or eliminated through the implementation of accepted security measures."

9. *Payments or gifts to respondents.* Respondents will not receive any payments or gifts aside from Enhanced A-CAM support if they comply with these requirements.

10. *Assurance of confidentiality.* Carriers' certifications will be made available for public inspection. Carriers may request that the cybersecurity and supply chain risk management plans they submit be withheld from public inspection by selecting the appropriate option when they submit their plans. *See* 47 CFR § 0.459(a)(4). However, if a request for public inspection is made under 47 CFR § 0.461, and the carrier has any objections to disclosure, the applicant will be notified and will be required to justify continued confidential treatment.

11. *Questions of a sensitive nature*. This information collection does not address any private matters of a sensitive nature.

12. *Estimates of the hour burden of the collection to respondents.*

a. Submission and Certification of Initial Cybersecurity and Supply Chain Risk Management Plans:

(1) Number of respondents: Approximately 450.

(2) Frequency of response: Once.

(3) Total number of responses per respondent: 1.

(4) Estimated time per response: On average 50 hours per response.

(5) Total annual hour burden: 22,500 hours.

50 hours per respondent for 450 respondents filing once. Total annual hour burden is calculated as follows:

450 respondents x 1 submission = 450 responses x 50 hours = **22,500 total annual hours**.

(6) Total estimate of in-house cost to respondents: $1,617,300. (22,500 hours x 71.88/hour).

(7) Explanation of calculation: The Commission estimates that applicants will use staff equivalent to a GS-14/Step 5 ($71.88/hour) Federal employee to complete and submit the application. 450 (responses) x 50 (hours to prepare submission) x $71.88/hour = $1,617,300.

b. Submission of Substantially Modified Cybersecurity and Supply Chain Risk Management Plans:

(1) Number of respondents: Approximately 450.

(2) Frequency of response: 450.

(3) Total number of responses per respondent: On occasion

(4) Estimated time per response: On average 10 hours per response.

(5) Total annual hour burden: 4,500 hours.

10 hours per respondent for 450 respondents filing on occasion. Total annual hour burden is calculated as follows:

450 respondents x 1 submission on average = 450 responses x 10 hours = **4,500 total annual hours**.

(6) Total estimate of in-house cost to respondents: $323,460. (4,500 hours x $71.88/hour).

(7) Explanation of calculation: The Commission estimates that applicants will use staff equivalent to a GS-14/Step 5 ($71.88/hour) Federal employee to complete and submit the application. 450 (responses) x 10 (hours to prepare application) x $71.88/hour = $323,460.

TOTAL NUMBER OF RESPONDENTS: 450.
TOTAL NUMBER OF ANNUAL RESPONSES: 900
TOTAL ANNUAL BURDEN HOURS: 27,000 HOURS

TOTAL ANNUAL "IN-HOUSE" COST to RESPONDENT: $1,940,760

13. *Estimates of the cost burden of the collection to respondents.* There is no external cost burden to the respondents. Carriers should not incur capital and start-up costs or operation and maintenance of purchase of services in connection with submitting and certifying cybersecurity and supply chain risk management plans.

TOTAL CAPITAL AND START-UP COSTS OR OPERATION AND MAINTENANCE (O&M) = $0.

14. *Estimates of the cost burden to the Commission.* There will be few, if any, costs to the Commission beyond normal labor costs because ensuring proper use of universal service support is already part of Commission duties.

15. *Program changes or adjustment.* This is a new information collection resulting in program change increases of 450 total respondents, 900 total annual responses, and 27,000 total annual burden hours will be added to OMB's Active Inventory due to the adoption of FCC 23-60.

16. *Collections of information whose results will be published.* As discussed above, the Commission will make any non-proprietary information publicly available on the Internet as the Commission deems appropriate.

17. *Display of expiration date for OMB approval of information collection.* The Commission seeks approval to not display the OMB expiration date on the portal that USAC uses to collect the certifications and plans from Enhanced A-CAM carriers. This will prevent the Commission from having to change the OMB expiration date whenever we re-submit this information collection for approval. The Commission will publish the OMB control number and OMB expiration date and title in the Code of Federal Regulations. *See* 47 CFR § 0.408.

18. *Explain any exceptions to the statement certifying compliance with 5 C.F.R. § 1320.9 and the related provisions of 5 C.F.R. §1320.8(b)(3).* There are no exceptions to the Certification Statement.

B. Collections of Information Employing Statistical Methods:

No statistical methods are employed.