

effective date of the federal rule, as indicated by the amendatory instructions to change the regulatory text in 40 CFR part 70, appendix A. See, e.g., 68 FR 74871 (December 29, 2003) (a direct final rule), 68 FR 65637 (November 21, 2003), and 77 FR 54382 (September 5, 2012).

The direct final rule published on December 23, 2022 (87 FR 78871) matches the effective date of the program with the publication date of the rule, which would give sources less than one year from the program effective date to submit their applications. The following amendatory instructions correct the effective dates in Section VI and the regulatory text in FR Doc. 2022–27725 appearing on pages 78871–78874 in the **Federal Register** of Friday, December 23, 2022:

#### VI. Final Action [Corrected]

■ 1. On page 78874, at the top of the first column, the text “If we do not receive timely adverse comments, this direct final approval will be effective without further notice on December 23, 2022.” is corrected to read “If we do not receive timely adverse comments, this direct final approval will be effective without further notice on February 21, 2023.”

#### Appendix A to Part 70—Approval Status of State and Local Operating Permits Programs [Corrected]

■ 2. On page 78874, in the middle of the third column, the text “(6) The District adopted revisions on October 14, 2021. The California Air Resources Board submitted revisions to the EPA on January 24, 2022. Approval is effective on December 23, 2022.” is corrected to read “(6) The District adopted revisions on October 14, 2021. The California Air Resources Board submitted revisions to the EPA on January 24, 2022. Approval is effective on February 21, 2023.”

Dated: January 26, 2023.

**Martha Guzman Aceves,**

*Regional Administrator, Region IX.*

[FR Doc. 2023–02138 Filed 2–3–23; 8:45 am]

**BILLING CODE 6560–50–P**

## FEDERAL COMMUNICATIONS COMMISSION

### 47 CFR Parts 2 and 15

[ET Docket No. 21–232 and EA Docket No. 21–233; FCC 22–84; FR ID 120432]

#### Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program

**AGENCY:** Federal Communications Commission.

**ACTION:** Final rule.

**SUMMARY:** In this document, the Federal Communications Commission (Commission) amends its rules related to equipment authorization to further secure our communications networks and supply chain from equipment that poses an unacceptable risk to national security of the United States or the security and safety of United States persons. The Commission implements revisions to the equipment authorization program to prohibit authorization of equipment that has been identified on the Commission’s Covered List—published pursuant to the Secure and Trusted Communications Networks Act of 2019—as posing an unacceptable risk to national security of the United States or the security or safety of United States persons, and the Commission prohibits the marketing and importation of such equipment in the United States. The Commission also addresses what constitutes “covered” equipment for purposes of implementing the equipment authorization prohibition that the Commission is implementing. The actions being taken comply with Congress’s directive in the secure Equipment Act of 2021 to prohibit authorization of “covered” equipment on the Covered List within one year of that Act’s enactment and to lay the foundation to prohibit the authorization of any additional “covered” equipment that may be added to the Covered List based on a determination that such equipment poses an unacceptable risk to national security.

**DATES:** Effective February 6, 2023.

**FOR FURTHER INFORMATION CONTACT:** Jamie Coleman, Office of Engineering and Technology, (202) 418–2705 or [Jamie.Coleman@FCC.gov](mailto:Jamie.Coleman@FCC.gov). For additional information concerning the Paperwork Reduction Act information collection requirements contained in this document, contact Nicole Ongele, (202) 418–2991 or send an email to [PRA@fcc.gov](mailto:PRA@fcc.gov).

**SUPPLEMENTARY INFORMATION:** This is a summary of the Commission’s document, Report and Order, and Further Notice of Proposed Rulemaking, ET Docket No. 21–232 and EA Docket No. 21–233; FCC 22–84, adopted November 11, 2022 and released November 25, 2022. The full text of this document is available for public inspection and can be downloaded at: <https://www.fcc.gov/document/fcc-bans-authorizations-devices-pose-national-security-threat>. When the FCC Headquarters reopens to the public, the full text of this document also will be available for public inspection and copying during regular business hours in the FCC Reference Center, 45 L Street NE, Washington, DC 20554. Alternative formats are available for people with disabilities (Braille, large print, electronic files, audio format) by sending an email to [FCC504@fcc.gov](mailto:FCC504@fcc.gov) or calling the Commission’s Consumer and Governmental Affairs Bureau at (202) 418–0530 (voice), (202) 418–0432 (TTY).

#### Procedural Matters

*Final Regulatory Flexibility Analyses.* The Regulatory Flexibility Act of 1980 (RFA) requires that an agency prepare a regulatory flexibility analysis for notice and comment rulemakings, unless the agency certifies that “the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities.” Accordingly, the Commission has prepared a Final Regulatory Flexibility Analysis (FRFA) concerning the possible impact of the rule changes contained in this Second Order on Reconsideration on small entities. As required by the RFA, an Initial Regulatory Flexibility Analysis (IRFA) was incorporated in the Notice of Proposed Rulemaking (NPRM) (86 FR 46644, August 19, 2021). The Commission sought written public comment on the proposals in the NPRM, including comments on the IRFA. No comments were filed addressing the IRFA. Accordingly, the Commission has prepared a Final Regulatory Flexibility Analysis (FRFA) concerning the possible impact of the rule changes contained in the document on small entities. The present FRFA conforms to the RFA and can be viewed under Appendix B of the item.

*Paperwork Reduction Act.* This document contains new and modified information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104–13. It was submitted to the Office of Management and Budget (OMB) for emergency review under section 3507(d) of the PRA. Public comment on this

submission has been waived pursuant to 5 CFR 1320.13(d). Amendments of parts 2 and 15 of the Commission's rules as set forth in Appendix A are effective on the date of publication in the **Federal Register**, including §§ 2.903(b), 2.911(d)(5), (6), and (7); 2.929(c); 2.932(e); 2.938(b)(2); 2.1033(b)(1), (2), (3), and (4); 2.1033(c)(1), (2), (3), and (4); 2.1043(b)(2)(i)(B), (C), (D), and (E); and 2.1043(b)(3)(i)(B), (C), (D), and (E), which contain new and modified information collection requirements that were reviewed and approved by the Office of Management and Budget (OMB) under the Paperwork Reduction Act, with an expiration date of June 30, 2023. The Office of Engineering and Technology establishes and announces the effective date of these sections in this document published in the **Federal Register**.

Because the emergency approval of this information collection has an expiration date of June 30, 2023, the Commission, as part of its continuing effort to reduce paperwork burdens and in the standard course of information collection review procedures, will issue a separate document inviting the general public to comment on the information collection requirements contained in this Final Rule as required by the Paperwork Reduction Act of 1995, Public Law 104–13. In addition, the Commission notes that pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107–198, see 44 U.S.C. 3506(c)(4), we previously sought specific comment on how the Commission might further reduce the information collection burden for small business concerns with fewer than 25 employees. The Commission has described impacts that might affect small businesses, which includes most businesses with fewer than 25 employees, in the Final Regulatory Flexibility Analysis (FRFA), and can be viewed under Appendix B of the item.

**Congressional Review Act.** The Commission has determined, and the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, concurs, that this rule is “non-major” under the Congressional Review Act, 5 U.S.C. 804(2). The Commission will send a copy of this document to Congress and the Government Accountability Office pursuant to 5 U.S.C. 801(a)(1)(A).

## Synopsis

### Background

In the *Notice of Proposed Rulemaking* (86 FR 46644, August 19, 2021) and *Notice of Inquiry* (86 FR 46641, August

19, 2021) (*NPRM* and *NOI*), the Commission proposed to revise its rules and procedures relating both to its equipment authorization program and its competitive bidding program to leverage the processes associated with these programs to help keep untrusted equipment and vendors out of U.S. networks. As the Commission made clear, the efforts underway in the instant proceedings are intended to be among the additional steps that the Commission is taking to be consistent with, and build upon, other efforts underway at the Commission, Congress, and the Executive Branch to protect our nation's supply chain from equipment and services that pose a national security risk or a threat to the safety of U.S. persons.

In March 2020, the Secure Networks Act was enacted. These provisions include: requiring (pursuant to section 2(a)) that the Commission publish, and periodically update, a list of “covered communications equipment and services” that have been determined to pose national security risks, requiring (per section 2(b)) that the Commission place on that list the equipment or services that are produced or provided by entities and meets certain capabilities, and further requiring (per section 2(c)) that the equipment or services placed on the list be “based solely on” determinations made by four enumerated sources. In particular, these determinations and sources are limited to—(1) a “specific determination made by any executive branch interagency body with appropriate national security expertise, including the Federal Acquisition Security Council . . . ;” (2) a “specific determination made by the Department of Commerce pursuant Executive Order No. 13873 . . . relating to securing the information and communications technology and services supply chain;” (3) the “communications equipment or service being covered telecommunications equipment or services, as defined in § 889(f)(3) of [the 2019 NDAA];” or (4) a “specific determination made by an appropriate national security agency.”

The Secure Networks Act also adopted other provisions. These included requiring the Commission to: prohibit any Federal subsidy made available through a program administered by the Commission that provides funds used for the capital expenditures necessary for the provision of advanced communications service to purchase or otherwise obtain or maintain “covered” communications equipment or services (section 3); establish the Secure Networks Act Reimbursement Program to make

reimbursements to certain advanced communications service providers to facilitate the removal, replacement, and disposal of certain “covered” communications equipment and services (section 4); and require each provider of advanced communications service to submit annual reports to the Commission regarding whether it has purchased, rented, leased, or otherwise obtained and “covered” communications equipment or services on or after August 14, 2018 or 60 days after new covered equipment and services are subsequently added to the Covered List (section 5).

Pursuant to the Secure Networks Act and § 1.50002(a) of the Commission's rules, PSHSB is required to publish the “Covered List,” which identifies “covered communications equipment or service” that has been determined, by one or more of four enumerated sources outside of the Commission, as posing an unacceptable risk to the national security of the United States or the security and safety of United States persons. The Commission tasked PSHSB with ongoing responsibilities for monitoring the status of the determinations and periodically updating the Covered List to address changes as appropriate.

On March 12, 2021, PSHSB published its first Public Notice on the Covered List. That list specifically identified equipment and services that, pursuant to the Secure Networks Act, had been determined by Congress in section 889(f)(3) of the 2019 NDAA—one of the four enumerated sources identified under the Secure Networks Act—as posing an unacceptable risk to national security. Among other things, that Covered List listed as “covered” equipment certain equipment produced by five different entities: Huawei, ZTE, Hytera, Hikvision, and Dahua (and their respective subsidiaries and affiliates).

On March 25, 2022, PSHSB published a Public Notice updating the Covered List; this list retained the earlier identified “covered” equipment (equipment produced by Huawei, ZTE, Hytera, Hikvision, and Dahua) while announcing additions to the Covered List based on new determinations by two of the other enumerated sources, DHS and an executive branch interagency body (Team Telecom) with appropriate expertise. Most recently, on September 20, 2022, PSHSB published another Public Notice updating the Covered List; this list also retained the earlier identified “covered” equipment (equipment produced by Huawei, ZTE, Hytera, Hikvision, and Dahua) while announcing certain additions to the Covered List based on new

determinations by the Department of Justice, in coordination and concurrence with the Department of Defense.

*The NPRM and NOI.* The Commission adopted an NPRM and an NOI on June 17, 2021. This initiated two separate dockets, with one docket concerning revisions to the Commission's equipment authorization program and the other concerning the Commission's competitive bidding program. In the NOI, the Commission sought broad comment on possible additional steps that it could take to leverage the equipment authorization program to promote cybersecurity.

*NPRM concerning the Equipment Authorization Program (ET Docket No. 21–232).* The Commission's equipment authorization rules play a critical role in enabling the Commission to carry out its responsibilities under the Communications Act. The Commission's equipment authorization program, codified in part 2 of its rules, promotes efficient use of the radio spectrum and addresses various responsibilities associated with certain treaties and international regulations, while ensuring that RF devices in the United States comply with the Commission's technical requirements before they can be marketed in or imported to the United States. As a general matter, for an RF device to be marketed or operated in the United States, it must have been authorized for use by the Commission, although a limited number of categories of RF equipment are exempt from this requirement.

In the NPRM, the Commission proposed to revise its equipment authorization program under its part 2 rules to prohibit authorization of "covered" equipment on the Commission's Covered List, *i.e.*, equipment that had been determined to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons. To achieve this goal, the Commission proposed to revise the rules and procedures for its two pathways for equipment authorization—certification and the supplier's declaration of conformity (SDoC). Recognizing that "covered" equipment might also include some equipment that is currently exempted from authorization requirements, the Commission sought comment on whether such exemptions should continue. The Commission also sought comment on whether any existing equipment authorization of "covered" equipment should be revoked, and if so, under what procedures. The Commission noted that adopting rules

that take security into consideration in the equipment authorization process would serve the public interest by addressing significant national security risks that had been identified, and would be consistent with the Commission's statutory "purpose of regulating interstate and foreign commerce in communications by wire and radio . . . for the purpose of the national defense [and] for the purpose of promoting safety of life and property." It tentatively concluded that the Commission has the authority to prohibit authorization of equipment on the Covered List, pointing to section 302 of the Communications Act of 1934, section 303(e), and other bases, including the Communications Assistance for Law Enforcement Act (CALEA), as well as ancillary authority under section 4(i) of the Act.

*NPRM on Competitive Bidding Program (EA Docket No. 21–233).* The Commission uses competitive bidding (*i.e.*, auctions) to determine which among multiple applicants with mutually exclusive applications for a license may file a full application for the license. Pursuant to this authority, the Commission has required each applicant that participates in competitive bidding to make various certifications. These required certifications address a range of public interest concerns related to the conduct of competitive bidding and the national security interest in precluding some parties from obtaining licenses through competitive bidding. Parties unable to make the required certifications have their applications to participate dismissed.

In the NPRM, the Commission sought comment on requiring any entity participating in the Commission's competitive bidding processes to certify that its bid does not and will not rely on financial support from any entity that the Commission has designated, under § 54.9 of its rules, as a national security threat to the integrity of communications networks or the communications supply chain. Under those existing rules, Huawei and ZTE and their parents, affiliates, and subsidiaries have been so designated.

*NOI on Equipment Authorization Program (ET Docket No. 21–232).* In the NOI, the Commission sought broad comment on other possible actions the Commission could take to create incentives in equipment authorization processes for improved trust through the adoption of cybersecurity best practices in consumer devices.

*The Secure Equipment Act of 2021.* On November 11, 2021, subsequent to the Commission's adoption of the

NPRM and NOI, the President signed and enacted into law the Secure Equipment Act of 2021 (Secure Equipment Act). This Act specifically concerns the Commission's equipment authorization program in the instant proceeding (ET Docket No. 21–232), in which the Commission has proposed prohibiting future authorizations of equipment on the Commission's Covered List published under section 2(a) of the Secure Networks Act. In section 2(a)(1), the Secure Equipment Act provides that, not later than one year after the date of its enactment, the Commission "shall adopt rules" in the [instant] proceeding."

## Discussion

In this proceeding, the Commission builds upon ongoing efforts by Congress, the Executive Branch, and the Commission to protect our nation's networks and supply chains from equipment and services that pose an unacceptable risk to national security or the safety of U.S. persons. Consistent with the Commission's proposals in the NPRM (ET Docket No. 21–232), the Commission implements several revisions to the Commission's equipment authorization program to prohibit authorization of "covered" equipment identified on the Commission's Covered List in order to protect our nation's communications systems from equipment that has been determined to pose an unacceptable risk. The Commission's actions in this proceeding fulfill Congress's mandate that the Commission adopt such rules within one year of enactment of the Secure Equipment Act of 2021. They also lay the foundation for future actions by the Commission to implement prohibitions in the equipment authorization program that will serve to protect the American people.

The Commission first finds that it has clear legal authority, as underscored by the Secure Equipment Act, for modifying the Commission's equipment authorization program to prohibit authorization of "covered" equipment identified on the Commission's Covered List. The Commission then discusses several rule revisions that it's adopting in the equipment authorization program (administered under part 2 of the Commission's rules) that will serve to prohibit the authorization of "covered" equipment, whether that equipment is listed on the current Covered List or is listed subsequently on an updated Covered List based on any future determinations made by our nation's national security agencies. The Commission also discusses the Covered

List, including the statutory framework associated with the list, the “covered” equipment on the current Covered List that the Commission is prohibiting from authorization, and how additional “covered” equipment identified in future updates to the Covered List will be prohibited from authorization under the Commission’s equipment authorization program. Finally, the Commission addresses other issues raised by commenters (e.g., cost-effectiveness and constitutional claims), as well as provide an overview of the Commission’s anticipated outreach efforts to inform manufacturers, industry, other interested parties, and the public that will be affected by the actions to protect the American public through elimination from the United States’ equipment supply chain of equipment that poses an unacceptable risk to national security.

#### *A. Legal Authority To Address Security Concerns Through the Equipment Authorization Program*

The Commission finds that it has authority to adopt the proposals in the *NPRM* with regard to prohibiting authorization of “covered” equipment on the Covered List. The Commission reaches this determination based on two grounds.

First, the Commission finds that the Secure Equipment Act provides the Commission with express authority to adopt rules that prohibit the review or approval of any application for equipment authorization for equipment that is listed on the Commission’s Covered List and requires the Commission to act. Section 2(a)(1) of the Secure Equipment Act expressly states that, no later than one year after its enactment, the Commission shall adopt rules in the instant proceeding to do so. By determining here—as specified in more detail below—that the agency will no longer review or approve any equipment authorization for equipment that is on the Commission’s Covered List, the Commission is acting based on the clear and express statutory language contained in section 2(a)(1) of the Secure Equipment Act. Thus, the Commission has legal authority to adopt those rules.

Second, the Commission has legal authority to take the relevant equipment authorization actions to prohibit authorization of “covered” equipment specified in the Report and Order (as well as with regard to revocation of authorizations discussed below) based on the agency’s statutory authority that predates Congress’s 2021 enactment of the Secure Equipment Act. Before that enactment, the Commission’s *NPRM* in

this proceeding relied on a number of preexisting statutory provisions to support this view. The Commission continues to believe, as noted in the *NPRM*, that section 302 of the Communications Act provides additional authority to adopt the rule and procedure changes proposed in the *NPRM*. The directive in section 302 to, “consistent with the public interest, convenience, and necessity, make reasonable regulations . . . governing the interference potential of devices which in their operation are capable of emitting radio frequency energy by radiation, conduction, or other means in sufficient degree to cause harmful interference to radio communications,” gives the Commission authority to implement other statutory responsibilities. And the inclusion of the phrase “public interest” in section 302(a) provides independent authority to take into account, in the Commission’s consideration of the public interest, the national defense, and the promotion of safety of life and property, goals which must inform the Commission’s exercise of its statutory responsibilities. As explained extensively in the Report and Order, prohibiting authorization of equipment that has been placed on the Covered List is essential to the national defense and to the promotion of public safety. It is well-established that the promotion of national security is consistent with the public interest and part of the purpose for which the Commission was created. As section 1 of the Act states, the Commission was created “for the purpose of the national defense [and] for the purpose of promoting safety of life and property through the use of wire and radio communication . . . .” And as the Supreme Court has instructed, the Commission does not read any “particular statutory provision in isolation,” but rather “in [its] context and with a view to [its] place in the overall statutory scheme.”

In this regard, as further noted in the *NPRM* issued prior to the Secure Equipment Act, the Commission’s statutory authority also included the authority under § 303(e) of the Communications Act to “[r]egulate the kind of apparatus to be used with respect to ‘its external effects’ (among other things). Further, as suggested in the *NPRM*, section 105 of the Communications Assistance for Law Enforcement Act (CALEA) supports the Commission’s authority to prescribe the rules that the Commission adopted in the Report and Order. That section requires telecommunications carriers to ensure that the surveillance capabilities

built into their networks “can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission,” and the Commission has concluded that its rule prohibiting the authorization of equipment on the Covered List that poses a national security threat implements that provision. The Commission is required to prescribe rules necessary to implement CALEA’s requirements, and the Commission concludes that the rules it implements here will help ensure that equipment that carriers include in their networks will not include such unlawful interception capabilities because use of equipment from companies that are identified by Congress and national security agencies to pose a national security threat is far more likely to be subject to unauthorized access. Finally, as noted in the *NPRM*, the Commission has ancillary authority to implement these statutory provisions by adopting such rules “as may be necessary in the execution of [these foregoing Commission] functions.”

The Commission’s reading of its pre-existing authority is confirmed by Congress’s enactment of the Secure Equipment Act. By specifying both this proceeding, by its docket number, in referring expressly to “the Notice of Proposed Rulemaking” pending before the Commission, and by directing the Commission to “clarify” that it would no longer review or approve any application for equipment that is on the Covered List, Congress clearly intended to ratify the Commission’s tentative conclusions in the *NPRM* that it had authority as discussed therein.

For all these reasons, the Commission now determines that it has the requisite legal authority to take these actions. Indeed, the argument to the contrary can be summarized as follows: even though the Commission has authority to approve equipment for use in the United States, the Commission has no statutory discretion to determine not to authorize that equipment in the event that a national security agency determines that the equipment poses an unacceptable risk to our national security. The Commission rejects the argument that the foregoing collective sources of statutory authority—in the absence of the Secure Equipment Act—would have deprived the Commission of such discretion. And Congress expressly endorsed this view in the Secure Networks Act.

### *B. Revisions to the Equipment Authorization Program*

In the *NPRM*, the Commission proposed to adopt revisions to its equipment authorization rules and processes to prohibit authorization of “covered” equipment on the Covered List. The Commission proposed or sought comment on several potential revisions to various rule provisions related to the equipment authorization processes that would implement the proposed prohibition on authorization of equipment on the Covered List. In particular, the Commission proposed or sought comment on revisions to the Commission’s general part 2 rules and to specific provisions relating to authorization of equipment processed through the Commission’s equipment certification and SDoC processes. The Commission notes at the outset that the Commission received numerous comments in support of its general objectives in proposing rules prohibiting authorization of equipment on the Covered List. Several of these and other commenters also offer particular views on how the Commission should implement the prohibition, and some oppose significant elements of the proposal. The Commission addresses the particular issues raised by commenters, below.

#### 1. General Provisions

In the *NPRM*, the Commission proposed to adopt, in the “General Provisions” section of its part 2, subpart J rules, a general prohibition of authorization of “covered” equipment identified on the Covered List. In particular, the Commission proposed to add new § 2.903 to clearly establish that the equipment on the Covered List—whether subject to the certification process or the SDoC process—would be prohibited from obtaining a Commission equipment authorization. The Commission sought comment on the proposal and whether modifications or clarifications of the proposed new rule were needed. In response, the Commission received one comment expressing general support and one of general opposition, largely arguing that the Commission lacks the authority to enact such a prohibition. As discussed in the Report and Order, Congress, through the Secure Equipment Act, directed the Commission to adopt rules, no later than November 11, 2022, to clarify that it would no longer review or approve any application for authorization of equipment on the Covered List. The Commission thus has an explicit statutory mandate to adopt such rules.

In accordance with the direction provided by the Secure Equipment Act, the Commission adopted new rule 2.903 in subpart J of the Commission’s part 2 equipment authorization rules. This general prohibition makes clear that “covered” equipment identified on the Covered List will no longer be eligible for either of the two Commission equipment authorization procedures—certification or SDoC. In accordance with section 2(d) of the Secure Networks Act, the prohibition will extend to any communications equipment that is included in an updated Covered List in the future, and will no longer extend to any communications equipment that is removed from the Covered List. As discussed further in the Report and Order, this new provision also serves to prohibit marketing such equipment under subpart I of the Commission’s rules and importation of such equipment under subpart K.

The Commission also includes within this new rule, additional general provisions associated with implementation of this prohibition in the Commission’s equipment authorization program under part 2. These provisions include definitions to be used in connection with the Covered List (e.g., “subsidiary” and “affiliate”), as well the requirement that OET and PSHSB publish and maintain on the Commission’s website information concerning on what constitutes “covered” equipment for purposes of implementing the prohibition on authorization of “covered” equipment.

#### 2. Certification Rules and Procedures

In the *NPRM*, the Commission proposed several revisions to various rules and procedures concerning the certification of equipment, and sought comment on other potential revisions, in order to ensure that equipment on the Covered List would no longer receive equipment authorization. The Commission noted that its intent is to revise the equipment authorization process in a way that efficiently and effectively prohibits authorization of “covered” equipment without delaying the authorization of innovative new equipment that benefits Americans’ lives. Thus, the Commission sought comment on “[w]hat information may be pertinent to assist the TCBs and the Commission in ensuring” against equipment authorization for such “covered” equipment, and on revisions to its rules that could better ensure compliance with those new requirements.

As explained in the *NPRM*, the equipment certification procedures

apply to certain radiofrequency devices that have the greatest potential to cause harmful interference to radio services. Certification generally is required for equipment that consists of radio transmitters as well as some unintentional radiators. Examples of equipment that requires certification include wireless provider base stations, mobile phones, point-to-point and point-to-multipoint microwave stations, land mobile, maritime and aviation radios, wireless medical telemetry transmitters, Wi-Fi access points and routers, home cable set-top boxes with Wi-Fi, and most wireless consumer equipment (e.g., tablets, smartwatches, and smart home automation devices).

Applicants for equipment certification are required to file their applications, which must include certain specified information, with an FCC-recognized Telecommunications Certification Body (TCB). The Commission, through its Office of Engineering and Technology (OET), oversees the certification process, and provides guidance to applicants, TCBs, and test labs with regard to required testing and other information associated with certification procedures and processes, including correspondence and pre-approval guidance provided via OET’s knowledge database system (KDB). Each applicant must provide the TCB with all pertinent information as required by the Commission’s rules, including documentation that addresses compliance with the testing requirements that broadly apply to RF devices, specific technical requirements in particular service rules, and other applicable policy-related Commission requirements. The TCB then evaluates the submitted documentation and test data to determine whether the device complies with the relevant Commission rules. Once a TCB grants an application, information about that authorization is publicly announced “in a timely manner” through posting on the Commission-maintained equipment authorization system (EAS) database, and referenced via unique FCC identifier (FCC ID). Certified equipment also is subject to various other requirements, including rules for modifying the equipment, marketing the equipment, and changing or transferring ownership of the associated FCC ID.

The Commission’s goal is to revise the equipment authorization process in a way that efficiently and effectively prohibits authorization of covered equipment without delaying the authorization of innovative new equipment that benefits Americans’ lives. In the *NPRM*, the Commission proposed and sought comment on a

requirement for each applicant for certification to make an attestation that the equipment is not “covered” equipment on the Covered List. It also asked whether the applicant should be required to provide specific additional information that would help establish that the equipment is not “covered.” In addition, the Commission proposed that the party responsible for ensuring that equipment complies with applicable requirements be located within the United States and that the application for certification include relevant contact and address information.

*Attestation requirement.* In the *NPRM*, the Commission specifically proposed to add a new provision to § 2.911 that would require applicants for certification to provide a written and signed attestation that, as of the date of the filing of the application, the equipment is not “covered” equipment produced by entities identified on the Covered List. The Commission proposed, further, that this attestation would encompass an attestation that no equipment, including any “component part,” is comprised of “covered” equipment. The Commission sought comment on whether such an attestation would be sufficient to implement the prohibition against authorization of covered equipment, the exact wording of the attestation, and the applicant’s responsibility related to any changes in the Covered List. In addition, the Commission asked whether it should require the applicant to provide, under § 2.1033, additional information (possibly including a “parts” list) that could help establish that the equipment is not “covered” in order to assist TCBs and the Commission in ensuring that applicants do not seek certification of “covered” equipment. Finally, in the *NPRM*, the Commission proposed to direct OET, working with other bureaus and offices across the Commission (including PSHSB, WCB, IB, and EB), to develop pre-approval guidance or other guidance for applicants and TCBs in order to implement the prohibition on authorization of “covered” equipment.

The Commission adopted a general attestation requirement in the form of a written and signed certification that the equipment is not prohibited from receiving an equipment authorization pursuant to new § 2.903. Specifically, the Commission revises § 2.911 to include a requirement that each applicant for equipment authorization in the certification process expressly provide a written and signed certification that, as of the date the applicant submits the required information to a TCB, the subject equipment is not prohibited from

receiving an equipment authorization pursuant to § 2.903.

The Commission also will require that each applicant indicate, as part of this certification, whether it is an entity identified on the Covered List with respect to “covered” equipment. The Commission notes that such entities on the Covered List could include entities specifically identified by name, as well as other associated entities, such as their subsidiaries and affiliates, and if so, then the applicant must indicate whether it is any such entity. The Commission finds that requiring submission of this additional information as part of the application for equipment certification will help ensure that prohibited “covered” equipment is not authorized. The rules that the Commission adopted to prohibit authorization of “covered” equipment rely in the first instance on the attestations by applicants at the beginning of the application process. Considering that applications for equipment certifications can be quite numerous, the Commission finds that knowing whether an applicant for equipment certification is an entity identified on the Covered List is essential to the efficient and effective administration by the Commission and the TCBs of the statutory prohibition in the Commission’s equipment authorization program. The Commission agrees with Motorola that transparency concerning the subsidiary or affiliate status of an applicant is important, and this requirement will facilitate such transparency. While the Commission notes that indicating that the applicant is an entity on the Covered List does not mean that the subject equipment qualifies as “covered” equipment as such, such information nonetheless can potentially assist the TCBs, as well as the Commission in the oversight, and will be another feature that will be integral to ensuring that “covered” equipment is not authorized. In sum, the Commission finds this requirement both reasonable and justified, particularly given the national security concerns related to preventing authorization of “covered” equipment and the directive of Congress in the Secure Equipment Act.

The Commission notes that the Covered List must be periodically updated, which will likely result in periodic modifications as to the equipment or entities identified on the Covered List. Implementing a general attestation requirement, as opposed to a specific provision that directly relates to the equipment identified on the current Covered List, provides the flexibility for accommodating potential changes in the

“covered” equipment on an updated Covered List. The Commission recognizes that there may be instances in which the Covered List is modified while an application for certification is pending. To ensure that the Commission adequately addresses such changes to the Covered List, the Commission adopted an additional requirement under § 2.911 specifying that, if the Covered List is modified after the date of the attestation but prior to grant of the authorization, then the applicant must provide a new written and signed certification that the subject equipment is not “covered” equipment identified on the Covered List as so amended.

Based on the record before us and the concerns raised, the Commission finds that any attestation that more broadly encompasses all “component parts” raises several issues that require additional consideration, and accordingly, the Commission seeks further comment on those issues in the Further Notice of Proposed Rulemaking in this proceeding. Thus, the Commission is not requiring, at this time, that the attestation specifically address individual component parts contained within the subject equipment, or provide any additional information in the application filed in accordance with § 2.1033.

The Commission will require that applicants for equipment certification, when attesting that their equipment is not “covered,” take into consideration the Commission’s definitions and guidance regarding what constitutes “covered” equipment, as separately discussed in more detail. Several commenters note the importance of clear guidance for purposes of the attestation requirement. This guidance, which will be posted on the Commission’s website, will be updated as appropriate to incorporate any further updates to the Covered List that affect “covered” equipment for purposes of the equipment authorization program, and will provide additional clarity regarding the requisite attestation. Attestations by each applicant that the subject equipment is not prohibited from receiving an equipment authorization must be true and accurate. As discussed below, in order to protect against abuse of the application process that relies on this attestation, the Commission also adopted new procedures for revoking equipment certifications for false statements or representations made by any applicant in its application for certification regarding “covered” equipment.

*Agent for service of process located in the United States.* In the *NPRM*, the Commission sought comment on actions

that it should take that would better ensure that equipment certification applicants and grantees comply with the requirements proposed in the *NPRM*. In particular, the Commission proposed requiring that the party responsible for compliance with the applicable requirements concerning certified equipment have a party located within the United States that would be responsible for compliance, akin to the current requirement applicable for equipment authorized through the SDoC process. The Commission also asked whether it should require the applicant for an equipment certification to identify an agent for service of process that must be located within the United States. Finally, the Commission sought comment on how much additional burden such requirements would place on the applicant and whether similar requirements should be placed on grantees of existing equipment authorizations.

The Commission continues to believe that it is important to facilitate enforcement of its rules, and the actions in this proceeding to prohibit future authorization of “covered” equipment that poses an unacceptable risk to national security underscore the need for effective enforcement of applicable rules associated with certified equipment. For many certified devices that are imported to and marketed in the United States, the grantees of the associated equipment authorizations are located outside of the United States. It is not always easy to communicate effectively with grantees, particularly foreign-based grantees, in order to engage in relevant inquiries, determine compliance, or even enforce the Commission’s rules where appropriate. Accordingly, the Commission believes it’s important to have a reliable and effective means to readily identify and contact a representative of the grantee of an FCC equipment certification.

Accordingly, in the Report and Order, the Commission adopted a requirement that each applicant for equipment certification designate a contact located in the United States for purposes of acting as its agent for service of process, regardless of whether the applicant is a domestic or foreign entity. The Commission believes that this requirement is straightforward, easy to implement, and should not place much of a burden on applicants seeking equipment authorization. However, as for the proposal to require that, for equipment certification, the party responsible for compliance be located in the United States, the Commission finds that defining specific requirements that the Commission should adopt and

implementing them within its processes raises more complicated issues. Thus, the Commission further concludes that it would benefit from further consideration of these issues in the Further Notice of Proposed Rulemaking portion of this proceeding.

An agent for service of process traditionally holds the obligation to accept the service of process and other documents on behalf of the party chiefly responsible, and to swiftly and dutifully deliver them to that party. Service of process includes, but is not limited to, delivery of any correspondence, notices, orders, decisions, and requirements of administrative, legal, or judicial process related to Commission proceedings. The rule the Commission adopted reflects other well-established service of process requirements in the Commission rules.

For purposes of implementing this requirement, the Commission revises its rules to require that the applicant for equipment certification include with its application for certification a written certification identifying the agent for service of process by name, U.S. physical address, U.S. mailing address (if different), email address, and telephone number. An applicant that is located in the United States may designate itself as the agent for service of process. The attachment designating the agent for service of process must include a statement, signed by both the applicant and its designated agent for service of process, if different from the applicant, acknowledging the applicant’s consent to accept service of process in the United States at the physical mailing address, U.S. mailing address (if different), and email address of its designated agent, as well as the agent’s acceptance of its obligation. Requiring that the agent expressly consent to service within the United States will enable the Commission to efficiently carry out its enforcement duties, and if the grantee is foreign-based, will facilitate enforcement without the need to resort to unwieldy procedures that may otherwise apply under international law. The written certification must also include the applicant’s acknowledgment that the designation of the agent must remain in effect for no less than one year after the grantee has terminated all marketing and importing of the associated certified equipment within the United States or the conclusion of any Commission-related administrative or judicial proceeding involving the equipment, whichever is later. In line with existing Commission rules, service is deemed to be complete when the document is sent to the U.S. physical address, U.S. mailing address (if different), or email

address of the U.S.-based agent for service of process. While, as discussed in the *NPRM*, the Commission sought comment on whether to apply such a requirement for an agent for service of process located in the United States to equipment already authorized pursuant to the certification process, the Commission declined to do so in the Report and Order unless there is a change in the name or address of the grantee or the grantee modifies the authorized equipment, as discussed immediately below.

*Modification of equipment, including permissive changes.* In the *NPRM*, the Commission sought comment on possible revisions to the part 2 rules to ensure that equipment users will not make modifications to existing equipment that would involve replacement with “covered” equipment. In particular, the Commission asked whether it should revise § 2.932 regarding modifications to equipment (e.g., changes in the design, circuitry, or construction of the device) or the § 2.1043 provisions concerning changes to certified equipment, such as “permissive changes.”

The Commission finds that, in order to fully implement the newly adopted prohibition on authorization of “covered” equipment the Commission must also revise § 2.932 concerning modification of equipment. A modification to authorized equipment could result in the later identification of that equipment as “covered.” the Commission cannot allow the continued authorization of modified equipment if, at the time of such modification, the equipment is “covered” equipment on the Covered List. Accordingly, the Commission adopted revisions to § 2.932 to require, similar to the revised provisions of § 2.911, that all applications or requests to modify already certified equipment include a written and signed certification that the equipment is not prohibited from receiving an equipment authorization pursuant to § 2.903. The Commission also requires an affirmative or negative statement as to whether the applicant is identified on the Covered List, as well as the written and signed certifications required under § 2.911(d)(6) regarding an agent for service of process within the U.S. Similarly, the Commission also adopted the same provisions for requests for Class II and III permissive changes pursuant to § 2.1043. The Commission finds that these revisions are sufficient to prevent modified equipment from maintaining authorization when such modifications occur at a time after which such equipment has been identified as posing



a risk and thereby appearing on the Covered List.

*Requirements that grantees update certain changes following grant of certification.* Considering that § 2.929 includes provisions regarding changes in the name, address, ownership, or control of the grantee of an equipment authorization, in the *NPRM*, the Commission also asked whether revisions were appropriate to that rule, consistent with the goals of this proceeding. Section 2.929 sets forth the requirements that the grantee of an equipment certification must maintain accurate, up-to-date contact information on file with the Commission:

“[w]henver there is a change in the name and/or address of the grantee of certification, notice of such change(s) shall be submitted to the Commission via the internet at <https://apps.fcc.gov/eas> within 30 days after the grantee starts using the new name and/or address.” The grantee also must report the assignment, exchange, or certain transactions affecting the grantee (e.g., transfer of control or sale to another company, mergers, and/or manufacturing rights), irrespective of whether the Commission requires a new application for certification. The current rule also permits a grantee to license or otherwise authorize a second party to manufacture the equipment. The Commission did not receive comments on updating § 2.929.

The Commission adopted revisions to § 2.929 in order to ensure that certain post-authorization changes do not result in that equipment becoming “covered” equipment that poses an unacceptable risk to national security. The Commission finds that certain changes in the name, address, ownership, or control of the grantee of an equipment authorization could result in previously authorized equipment being produced by an entity identified on the Covered List as producing “covered” equipment, thus resulting in the equipment becoming “covered” equipment. Accordingly, the Commission revises the requirements in § 2.929 to ensure that a grantee cannot circumvent the prohibition on authorization of equipment on the Covered List by transferring ownership or control, or licensing or otherwise authorizing a second party to manufacture the equipment associated with the grant of the equipment authorization. Specifically, the Commission revises § 2.929 to prohibit the grantee of an equipment authorization from licensing or otherwise authorizing a second party to manufacture the equipment covered by the grant of the equipment authorization if such licensing or

authorization would result in the equipment falling within the scope of “covered” equipment. The Commission further adopted a requirement that notice of any change in the name or address of the grantee of certification, or transactions affecting the grantee (such as a transfer of control or sale to another company, mergers, or transfer of manufacturing rights), include provisions similar to the revised provisions of § 2.911. Specifically, the Commission requires that the notice include a written and signed certification that as of the date of the filing of such notice, the equipment to which the change applies is not prohibited from receiving an equipment authorization pursuant to § 2.903. The Commission also requires that the notice include an affirmative or negative statement as to whether the grantee is identified on the Covered List (e.g., is subsidiary or affiliate of an entity named on the Covered List as producing “covered” equipment).

The Commission also revises § 2.929 to help ensure compliance with the effective service of process requirement added to § 2.1033, described above. For the same reasons that the Commission requires a U.S.-based agent for service of process for applicants, the Commission will require that the grantee maintain an agent for service of process that is located in the United States. Therefore, the Commission adds to § 2.929 the requirement that grantees must report any change to the information of the designated U.S.-based agent for service of process in updating the information on file with the Commission along with the written and signed certifications required under new § 2.911(d)(7).

*Conforming edits in part 2.* The Commission makes several conforming edits in the part 2 rules to reflect the requirements that the Commission adopted in the Report and Order. Several part 2 rules are revised, as appropriate to reflect that the requirements for equipment authorization now include the responsibility to comply with non-technical requirements such as the Covered List prohibitions. The Commission notes that it also adopted in § 2.1033 the provisions adopted in § 2.911(d) to clarify that the required information must be provided with the application for certification.

*Other issues raised in the NPRM.* In the *NPRM*, the Commission sought comment on other possible steps that it should consider that would affect its certification rules, such as actions that could be taken following grant of an equipment authorization that might be helpful in enforcing the prohibition on

authorization of “covered” equipment. These included whether the Commission should consider adopting any post-grant review procedures following the grant of an equipment authorization, or any revisions or clarifications concerning “post-market surveillance” activities with respect to products that have been certified. In the few comments the Commission received on these issues, most opposed any changes, and the Commission is not at this time adopting any revisions or clarifications to the Commission’s rules on these issues. The Commission does, however, think they merit further consideration, particularly now that the Commission has adopted a specific set of rules and procedures prohibiting authorization of “covered” equipment. Accordingly, the Commission seeks further comment in the Further Notice portion of this proceeding, requesting comment in light of the rule revisions that the Commission adopted in the Report and Order.

### 3. Supplier’s Declaration of Conformity (SDoC) Rules and Procedures

In the *NPRM*, the Commission proposed that any equipment produced by any of the entities (or their respective subsidiaries or affiliates) that produce covered equipment, as specified on the Covered List, would no longer be authorized pursuant to the Commission’s SDoC processes, and that the equipment of any of these entities would be subject to the Commission’s certification process. Under this approach, responsible parties would be prohibited altogether from relying on authorization using the SDoC process with respect to any equipment produced or provided by these entities (or their respective subsidiaries or affiliates), as such equipment could not be authorized utilizing the SDoC process. The Commission sought to ensure consistent application of its prohibition on further authorization of any “covered” equipment by requiring a single process, the certification process, which involves more active Commission oversight than the SDoC process for equipment produced by any entity identified on the Covered List as producing “covered” equipment. The Commission also invited comment on the specific information that should be included in the SDoC compliance statement that would ensure that responsible parties do not use the SDoC process for equipment produced by entities identified on the Covered List as producing “covered” equipment.

As discussed in the *NPRM*, the SDoC procedures, which are available for specific equipment generally considered



to have reduced potential to cause harmful RF interference, permits equipment to be authorized through reliance on the responsible party's self-declaration that the equipment complies with the pertinent Commission requirements. Accordingly, the SDoC process differs significantly from the certification process, and does not involve the more active and transparent oversight of the certification process. Many devices eligible for an SDoC authorization do not contain a radio transmitter and include only digital circuitry (e.g., computer peripherals; microwave ovens; industrial, scientific, and medical (ISM) equipment; switching power supplies; light-emitting diode (LED) light bulbs; radio receivers; and TV interface devices), although an SDoC authorization is also permitted for certain transmitters used in licensed services. As the Commission noted, under existing rules, the use of SDoC procedures are "optional," as each responsible party for an SDoC-eligible device could choose to obtain equipment authorization using either certification or SDoC procedures.

For each particular RF device, the completion of the SDoC process signifies that the responsible party affirms that the necessary measurements have been made, or other procedures that have been found acceptable to the Commission have been completed, to ensure that the particular equipment complies with the applicable requirements. As set forth in the Commission's rules, the responsible party may be the equipment manufacturer, the assembler (if the equipment is assembled from individual component parts and the resulting system is subject to authorization), or the importer (if the equipment by itself or the assembled system is subject to authorization), or, under certain circumstances, retailers or parties performing equipment modification. For devices subject to SDoC, the information the responsible party must keep on file includes a compliance statement that lists a U.S.-based responsible party. The SDoC process is "streamlined" in the sense that, unlike the certification process, it does not require submission of applicable information to a Commission-recognized TCB or the use of an FCC-recognized accredited testing laboratory. However, the Commission can specifically request that a responsible party provide compliance documentation or device samples as necessary.

*Prohibition on use of SDoC process for entities producing "covered" equipment on the Covered List.* In proposing in the *NPRM* that equipment

produced by any of the entities (or their respective subsidiaries or affiliates) identified on the Covered List as producing "covered" equipment would no longer be authorized pursuant to the Commission's SDoC process, the Commission sought to ensure consistent application of its proposed prohibition on authorization of "covered" equipment. The Commission contends that by shifting such equipment to the certification process, which involves more active oversight, including proactively providing guidance when working directly with TCBs prior to any equipment authorization, it would facilitate more effective post-market surveillance as appropriate. Because the Commission does not have direct involvement in the SDoC process (e.g., nothing is filed with or recorded by the Commission), that process presents significant additional challenges to ensure that covered equipment that might otherwise be eligible for the SDoC process does not make its way into the U.S. market.

The Commission is not persuaded by opponents of the proposal who assert that it is unnecessarily burdensome. Entities following either the certification or the SDoC process must both prove compliance with FCC rules through testing and supporting documentation. Given that information on equipment authorized via the SDoC process is not readily transparent to the Commission, the certification process provides the Commission with the necessary oversight to ensure that the Commission is achieving the goals in this proceeding to prohibit authorization of equipment that poses an unacceptable risk, as required by the Secure Equipment Act, and will help prevent "covered" equipment from improper authorization through the SDoC process in the first place. The Commission finds that it is appropriate and reasonable to foreclose the SDoC process to equipment produced by any entity identified on the Covered List as producing "covered" equipment and require equipment authorization through the certification process. The Commission adopted as proposed a rule prohibiting any of the entities identified on the Covered List as producing "covered" equipment from using the SDoC process to authorize any equipment—not just "covered" equipment identified on the Covered List. Thus, any equipment eligible for equipment authorization that is produced by any entity so identified on the Covered List must be processed pursuant to the Commission's certification process, regardless of any

Commission rule that would otherwise permit use of the SDoC process.

As explained in the *NPRM*, the Commission believes that requiring use of only one process by entities that have already been determined to produce "covered" equipment will serve the important goal of ensuring consistent application of the Commission's newly adopted prohibition on further authorization of any "covered" equipment, while also providing for more active oversight. Considering the importance of prohibiting equipment for devices that pose an unacceptable risk to national security, and that this is the Commission's first foray into implementing rules and procedures that require effective identification and prohibition of equipment that poses an unacceptable risk to national security, the Commission finds this approach at this time is consistent with the public interest. The Commission notes that, as the Commission, industry, and manufacturers gain more experience over time on the effectiveness of its SDoC procedures concerning "covered" equipment, the Commission may revisit this process.

*Attestation requirement.* In the *NPRM*, the Commission sought comment on what information should be included in the SDoC compliance statement to ensure that responsible parties do not use the SDoC process to authorize "covered" equipment. In the Commission's view, this compliance statement would need to be sufficiently complete to ensure that a responsible party exercises the necessary diligence to confirm that equipment that is subject to the SDoC process is not "covered" equipment for purposes of equipment authorization. Further, the Commission indicated that this compliance statement should be crafted in such a manner as to assist responsible parties in ensuring authorization is achieved through the appropriate process by identifying equipment produced by any entity identified on the Covered List as producing "covered" equipment, which can no longer be authorized through the SDoC process. This statement would also ensure that responsible parties are held accountable, by their compliance statement, for any misrepresentations or violation of the prohibition that the Commission adopted.

As the Commission did for the certification process, the Commission adopted a general attestation requirement in the form of a written and signed certification that the equipment is not produced by any entity identified on the Covered List as producing "covered" equipment, pursuant to § 1.50002 of the Commission's rules.

Specifically, the Commission revises § 2.938 to include a requirement that the responsible party maintain record of a written and signed certification that, as of the date of first importation or marketing, the equipment for which the responsible party maintains Supplier's Declaration of Conformity is not produced by any entity that is identified on the Covered List as producing "covered" equipment. The Commission finds that the existing SDoC operational framework, in which the responsible party declares that the equipment complies with the pertinent Commission requirements, in concert with an explicit attestation by each responsible party completing the SDoC process that the subject equipment is not produced by any entity identified on the Covered List as producing "covered" equipment, pursuant to § 1.50002 of the Commission's rules, should be sufficient to render unlikely the possibility that equipment required to be processed through the Commission's certification procedures will instead be erroneously processed under the Commission's SDoC procedure. The Commission finds that JVCKenwood's suggestions that the attestation include other considerations beyond whether the equipment is "covered" (e.g., an attestation that the equipment was not unlawfully acquired) are beyond the scope of the Commission's proposal in this proceeding.

The required attestation by the responsible party for each device authorized under SDoC is similar to that required of applicants in the certification process. As with the attestation included in a certification application, the Commission will require a simple attestation here that the equipment is not produced by an entity identified on the Covered List as producing "covered" equipment, pursuant to § 1.50002 of the Commission's rules. The Commission does not believe that such a requirement will present an undue burden when weighed against the potential security risks described by Congress nor should it present any delay in authorizing equipment through the SDoC process. Such an attestation will also provide a mechanism for the Commission to, as needed, verify the origin of equipment authorized by SDoC and ensure accountability for a responsible party dealing with equipment provided by entities on the Covered List. The Commission expects that these measures will be sufficient to deter responsible parties from seeking the SDoC process for authorization of

equipment on the Covered List, and the Commission will rely on the enforcement procedures to ensure compliance. The Commission notes that the current rules require that the SDoC responsible party be located within the United States, and that the party's name, address, and telephone number or internet contact information be included in the compliance information that is provided with authorized equipment, and the Commission does not alter this requirement.

**Enforcement.** In the NPRM, the Commission also asked several questions relating to enforcement of the SDoC prohibitions and related requirements. In this regard, the Commission noted its existing authority to request equipment samples and compliance information, and asked questions about the circumstances that would warrant Commission requests and what information would be useful in proving/disproving such compliance. The Commission received no comments or suggestions on how it should approach these issues.

As noted in the NPRM, the Commission already has the authority to request that the responsible party provide information regarding any equipment that has been authorized through the SDoC procedures. Accordingly, the Commission will exercise oversight, as appropriate, by requesting that the responsible party provide relevant information—e.g., an equipment sample, representative data demonstrating compliance, and the compliance statement itself, including the attestation (in the form of a written and signed certification) required by this action, and any information necessary to assess the validity of that attestation—regarding any equipment that the Commission deems requires confirmation of its compliance with the rules. As with equipment authorized through the certification process, the Commission will take any available enforcement action to ensure that equipment identified on the Covered List does not receive equipment authorization and to hold accountable any entity that fails to accurately attest that any equipment for which they seek authorization is "covered" equipment. The Commission also will work with their federal partners to identify and block the importation of "covered" equipment that is placed on the Covered List and is prohibited from equipment authorization pursuant to the rules adopted in the Report and Order.

Finally, in light of the newly established SDoC rules and procedures to prohibit authorization of "covered" equipment, the Commission invites

further comment in the Further Notice of Proposed Rulemaking on other actions the Commission should consider when carrying out its responsibilities to ensure compliance with the prohibitions on authorization of "covered" equipment that the Commission adopted in the Report and Order.

#### 4. Importation and Marketing Rules

As the Commission noted in the NPRM, if it adopted its proposal to revise the Commission's subpart J equipment authorization rules to prohibit any further authorization of covered equipment through the certification or SDoC processes, this decision also would prohibit the marketing of such equipment under subpart I of the Commission's part 2 rules (Marketing of Radio-Frequency Devices) and importation of equipment under subpart K (Importation of Devices Capable of Causing Harmful Interference) of the part 2 rules. In the NPRM, the Commission sought comment on whether to revise or provide clarification with regard to how the proposal to prohibit authorizing covered equipment would affect the Commission's rules in either subpart I or subpart K. Specifically, the Commission asked whether the general prohibition it proposed for equipment subject to certification and SDoC made any changes to subparts I or K unnecessary and, if not, what changes were needed to the rules in those subparts.

The Commission affirms the conclusion that revising the general equipment authorization provisions in subpart J also effectively prohibits the marketing and importation of "covered" equipment prohibited from authorization under the equipment authorization program. Section 2.803(b) only permits persons to market RF devices that are subject to authorization under either the certification or SDoC process, as set forth in the Commission's subpart J rules, once those devices have been authorized, unless an exception applies. Similarly, the revisions in this proceeding to the equipment authorization process in subpart J, above, also prohibits importing or marketing of covered equipment if it is subject to authorization through either the certification or SDoC process in subpart J and has not been authorized, per §§ 2.1201(a) and 2.1204(a).

The Commission recognizes that commenters have raised points related to technical concerns and the intended use of imported equipment. However, as with the other rule revisions that the Commission adopted in the Report and

Order, the Commission focuses review of the importation and marketing rules on how they relate to addressing equipment on the Covered List in terms of equipment authorization. The Commission emphasizes that, generally under the rules, RF devices may be imported only when certain conditions are met. Many of those conditions are based on equipment authorization, with other very limited conditions based on personal use, demonstration, and other very restrictive conditions. As such, the Commission found that, there was no need to adopt revisions to the importation or marketing rules to address equipment on the Covered List because the revisions to the equipment authorization rules prohibiting any further authorization of covered equipment also serve to prohibit the importation and marketing of such equipment.

#### 5. Exempt Equipment

As a general matter, the Commission's equipment authorization program is concerned with ensuring that RF emissions do not cause harmful interference to radio communications. However, in the *NPRM*, the Commission recognized that this proceeding involves concerns about equipment that poses an unacceptable risk to our nation's communications networks, which are distinct from the Commission's concerns related to interference to authorized radio services. Asking whether "covered" equipment potentially could include equipment that currently is exempt from its equipment authorization processes, the Commission sought comment on whether to reconsider whether, in order to address security concerns, providing such exemptions continues to be appropriate.

**Background.** The most diverse set of exempt devices operate under the Commission's part 15 unlicensed device rules. Certain unlicensed RF devices are exempt from demonstrating compliance under either of the Commission's equipment authorization procedures (certification or SDoC) because these devices generate such low levels of RF emission that they have little potential for causing harmful interference to authorized radio services, although some devices may be exempt for other reasons. In addition, certain equipment that operates within licensed services are also exempt from part 2 equipment authorization due to a variety of reasons beyond interference concerns and are not subject to the Commission's specific part 2 testing, filing, or record retention requirements. However, such devices are subject to complying with the

unique operational and technical requirements associated with the particular licensed service.

In the *NPRM*, the Commission sought specific comment on whether the Commission should revise its rules to eliminate any equipment authorization exemption for "covered" equipment based on the potential of such equipment, regardless of RF emissions characteristics, to pose an unacceptable risk to U.S. networks or users. The Commission further sought comment on whether such a revision should apply only to exempt part 15 unlicensed devices or should include currently exempt devices that operate under other rule parts. The Commission also asked whether to require that any equipment (in whole or in part), regardless of any applicable rule exemption, that is produced by any entity that has produced "covered" equipment on the Covered List be processed pursuant to the Commission's certification process (similar to the proposal and the requirement that the Commission is adopting that such entities must use the certification process for equipment, even if existing rules had permitted processing through the SDoC process).

In the *NPRM*, the Commission tentatively concluded that the legal authority associated with the Commission's proposal to prohibit authorization of "covered" equipment in its equipment authorization process also provided, pursuant to sections 302 and 4(i) of the Act, for actions that the Commission might take with respect to precluding "covered" equipment from being exempted from the equipment authorization process.

**Discussion.** The Commission concludes that it will no longer exempt "covered" communications equipment, *i.e.*, equipment that has been determined to pose an unacceptable risk to national security pursuant to the Secure Networks Act, from equipment authorization requirements. Accordingly, the Commission will require that any equipment produced by any of the entities identified on the Covered List as producing "covered" equipment be processed through the certification process just as the Commission is requiring equipment previously subject to the SDoC procedures to be processed through the certification processes. By no longer exempting equipment produced by these entities, the Commission is taking another step to protect our nation's supply chain from new equipment that has been determined to be "covered."

As noted in the *NPRM*, certain RF equipment for various reasons has been exempted from the need to demonstrate

compliance under the Commission's equipment authorization procedures, which are generally concerned with ensuring that devices do not cause harmful interference to authorized radio services. Also as discussed in the *NPRM*, this proceeding involves concerns about equipment that poses an unacceptable risk to our nation's communications networks, which are distinct from the Commission's concerns related to harmful interference to authorized radio services. Whether communications equipment poses an unacceptable risk to national security simply does not turn on considerations of RF interference. Nor is the Secure Networks Act or Secure Equipment Act so concerned.

The Commission concludes that certain types of equipment that is currently exempt from equipment authorization requirements and produced by entities identified on the Covered List could constitute "covered" equipment. Later in this document, the Commission discusses certain types of communications equipment that is "covered" equipment. Among other things, the Commission concludes that, for purposes of implementing the prohibition on "covered" equipment, such equipment includes "access layer," "distribution layer," and "core layer" equipment produced by entities identified on the Covered List and that is used in networks providing advanced communications services. Pursuant to section 5 of the Secure Networks Act, the Commission requires that advanced communications service providers report whether they have purchased, leased, rented, or otherwise obtained such "covered" equipment (after August 18, 2018). "Access layer" equipment is equipment associated with providing and controlling end-user access to the network over the "last mile," "local loop," or "to the home" (*e.g.*, optical terminal line equipment, optical distribution network devices, customer premises equipment (to the extent owned by the advanced services provider), coaxial media converters, wavelength-division multiplexing (WDM) and optical transporting networking (OTN) equipment, and wireless local area network (WLAN) equipment). "Distribution equipment" includes middle mile, backhaul, and radio area network (RAN) equipment (*e.g.*, routers, switches, network security equipment, WDN and OTN equipment, and small cells). "Core layer" equipment is associated with the backbone infrastructure (*e.g.*, optical networking equipment, WDN and OTN, microwave equipment, antennas, RAN

core, Cloud core, fiber, and data transmission equipment). Thus, to the extent that equipment currently exempt from equipment authorization procedures is produced by any entity identified on the Covered List, such equipment will no longer be eligible for such exemption and must seek authorization through the certification process, and the Commission will revise the part 15 rules to so indicate.

Similar to the Commission's decision to no longer permit these entities to avail themselves of the SDoC process, requiring all equipment they produce to undergo more rigorous scrutiny as well as complying with the attestation requirements is the best way the Commission can fulfil its statutory obligation to ensure that "covered" equipment is no longer able to be purchased and used, thereby protecting national security. The Commission further concludes that the measures that it's taking are consistent with long-standing legal authority (as discussed above) and are reasonable and appropriate both to prohibit authorization of "covered" equipment on the Covered List pursuant to the Secure Networks Act and to further comply with Congress's mandate in the Secure Equipment Act.

#### 6. Revocation of Authorizations of "Covered" Equipment

In the *NPRM*, the Commission sought comment on revocation of equipment authorizations on the grounds that the equipment authorization involved "covered" equipment. The Commission tentatively concluded that, if it adopted new rules prohibiting authorization of "covered" equipment, the Commission had the authority to revoke any authorization that may have been granted after adoption of such rules based on applicants' false statements or representations that the equipment was not "covered." The Commission also tentatively concluded that the current rules provide the Commission with the authority to revoke any *existing* equipment authorizations—*i.e.*, authorizations granted before adoption of rules in this proceeding prohibiting any future authorization of "covered" equipment—if such equipment constituted "covered" equipment, and sought comment on whether there are particular circumstances that would merit revocation of any specific equipment authorization(s) and, if so, the procedures that should apply (including whether to adopt possible revisions to the current procedures).

With respect to equipment authorized subsequent to adoption of proposed rules prohibiting authorization of

"covered" equipment, the Commission tentatively concluded that § 2.939(a)(1) and (2) applied to "covered" equipment, such that the Commission could revoke any equipment authorization that may have been granted based on false statements or representations in the application for authorization attesting that the equipment is not "covered." Under this proposed approach, the Commission would revoke any such equipment authorization granted after adoption of the rules proposed in the *NPRM*, even if the TCBs or the Commission had not acted to set the grant aside within the 30-day period following the posting of the grant on the EAS database. In addition, the Commission tentatively concluded that, pursuant to § 2.239(a)(3), if authorized equipment is subsequently changed (*e.g.*, the responsible party initiates a permissive change which changes the equipment status from not covered to "covered" equipment), that equipment authorization could be revoked because such a change would violate the Commission's newly adopted prohibition on authorization of "covered" equipment.

As for revocation of any existing equipment authorizations involving "covered" equipment, the Commission sought comment on whether § 2.939(a)(4), which allows revocation "[b]ecause of conditions coming to the attention of the Commission which would warrant it in refusing to grant an original application" would provide the Commission basis for revoking equipment granted prior to adoption of the prohibition on authorization of "covered" equipment. In addition, the Commission tentatively concluded that if it were to adopt rules prohibiting authorization of "covered" equipment, then § 2.939(c), which states that the Commission "may also withdraw any equipment authorization in the event of changes in its technical standards," could constitute such a change in technical standards that warrants withdrawal of the equipment authorizations.

To the extent the Commission sought to revoke any equipment authorizations, it noted the current procedures set forth in § 2.939(b), and requested comment on whether it should use these specific procedures or other procedures, and on what process the Commission could use to help identify equipment authorizations for revocation. Finally, the Commission asked whether it should make any revisions to § 2.939, including whether that section should specifically address the revocation process for "covered" equipment.

The Secure Equipment Act, enacted subsequent to the close of the comment period on the *NPRM*, includes specific provisions concerning the Commission's actions that concern revocation of equipment authorizations involving "covered" equipment. In section 2(a)(2), Congress directed the Commission to adopt new rules prohibiting authorization of "covered" equipment. As for revocation of existing equipment authorizations involving "covered" equipment, section 2(a)(3)(A) of the Act provides that "[i]n the rules adopted" by the statutory deadline, the Commission "may not provide for review or revocation of any equipment authorization" granted before the adoption date of such rules. Section 2(a)(3)(B), however, provides generally that, other than in "the rules adopted" by the statutory deadline, the Secure Equipment Act does not prohibit the Commission from examining the necessity of review or revocation of any equipment authorization on the basis of the equipment being on the Covered List or adopting rules providing for any such review or revocation.

In the Report and Order, the Commission did not adopt any rules providing for the review or revocation of any currently existing equipment authorization granted prior to adoption of the Report and Order. With respect to equipment authorized after adoption of the Report and Order prohibiting authorization of "covered" equipment, the Commission adopted streamlined revocation procedures to apply if the authorization had been granted based on false statements or representations in the applications that the equipment is not "covered," or if the authorized equipment is modified or changed in such a way as to become "covered" equipment. In addition, the Commission concludes that it has the authority, as affirmed by Congress in the Secure Equipment Act, to consider the necessity to review or revoke an existing authorization of "covered" equipment approved prior to adoption of the Report and Order, and that it has such authority to consider such action without considering additional rules providing for any such review or revocation of existing authorizations.

*Streamlined revocation of authorizations based on false statements or representations about "covered" equipment.* With regard to revocation of equipment authorizations granted after adoption of rules prohibiting authorization of "covered" equipment, the Commission concludes, as in the *NPRM*, that the Commission already has authority, under its current rules in § 2.939(a)(1), to revoke

authorizations if the Commission discovers, post-authorization, that the application (or in materials or responses submitted in connection therewith) contained false statements or representations. The Commission notes that revoking authorizations on this basis is clearly permitted under the Secure Equipment Act, which did not proscribe adopting rules for revocation of authorizations that are granted after adoption of the Report and Order.

However, because Congress established that “covered” equipment poses an unacceptable risk to national security, the Commission finds that it is necessary to adopt an expedited mechanism for review and revocation of equipment authorizations that were granted after adoption of the Commission’s prohibitions where the application for such authorization contained a false statement or representation regarding the “covered” status of such equipment at the time of such statement or representation. To that end, the Commission adopted a new provision, § 2.939(d), providing for streamlined procedures to address such situations, as discussed further below.

Nothing in the Commission’s statutory authority requires that the process for revocation of equipment authorizations be conducted pursuant to existing rule § 2.939(b), *i.e.*, the revocation process generally afforded radio licensees. As the Commission noted in its 2020 order adopting streamlined procedures for certain administrative hearings, the hearing provisions in the Communications Act do not expressly require formal hearings (*e.g.*, hearings conducted with live witness testimony and cross examination and the introduction of evidence before a presiding officer). Instead, revocation proceedings generally are subject only to informal adjudication requirements under the Administrative Procedure Act, which requires that an authorization holder be given written notice of the facts or conduct which may warrant the revocation and an opportunity to demonstrate or achieve compliance with all lawful requirements. The Commission may resolve disputes of fact in an informal hearing proceeding on a written record. Thus, the Commission concludes that, going forward, where the Commission has reason to believe that an equipment authorization was granted on the basis of a false statement or representation by the applicant concerning whether the subject equipment is “covered” equipment, the more streamlined informal hearing procedures described below, based on a written record, will

apply. However, the Commission may in its discretion determine to hold oral hearings when needed to resolve a genuine dispute as to an outcome-determinative fact, and such hearings may be limited to testimony and cross-examination necessary to resolve that dispute.

As discussed in this document above, the Commission also is prohibiting the modification of equipment if such modification would alter the equipment’s status such that it would become “covered” equipment. In implementing this prohibition, the Commission requires that applications or requests to modify already certified equipment include a written and signed certification that the equipment is not “covered.” The Commission concludes that, pursuant to existing § 2.939(a)(3), the Commission already has authority to revoke an equipment authorization granted after the adoption of rules in the Report and Order if that equipment is changed in the future in such a way as to become “covered” equipment. Again, because “covered” equipment poses an unacceptable risk to national security, the Commission also will include within the streamlined procedures the authority to revoke equipment authorization in which equipment is changed in such a way that it becomes “covered” equipment where the application or request for modification is found to include false statements or representations that the equipment is not “covered.”

*Streamlined procedures.* In cases in which OET and PSHSB, working with other Bureaus/Offices as may be appropriate, have reason to believe that a particular equipment authorization or modification of an equipment authorization granted after adoption of the rules in the Report and Order was or may have been based on a false statement or representation made by an applicant, either in the application or in the materials connected therewith, regarding the required attestations under revised § 2.911 concerning whether the equipment was “covered” or whether the applicant is an entity identified on the Covered List, OET and PSHSB will investigate whether such authorization was improperly granted or otherwise should be revoked. OET and PSHSB will provide written notice to the equipment authorization holder of the initiation of a revocation proceeding and the grounds under consideration for such revocation. As discussed above, the Commission is requiring that applicants for equipment authorization make certain attestations under § 2.911 regarding the subject equipment in the context of “covered” equipment. False

statements or representations with respect to the application under this section provide grounds for revocation of the authorization pursuant to § 2.939(a)(1).

The Commission will model this procedure along lines consistent with section 558 of the Administrative Procedure Act. OET and PSHSB will issue an order to show cause why revocation proceedings should not be initiated, which order will provide notice of the facts or conduct which may warrant revocation, and an opportunity to demonstrate or achieve compliance. The equipment authorization holder will have 10 days thereafter to provide a written submission responding to the notice of proposed revocation. After reviewing the record and any supplemental information requested by OET and PSHSB, if they find that the equipment is “covered” or that the applicant did not disclose that it was an entity identified on the Covered List, they will initiate revocation proceedings, providing the basis for such decision. The Commission notes that the determination as to whether to revoke an authorization focuses on whether the attestation was true, and it does not require any finding that the applicant has the specific intent to make a false statement or representation. In the event of revocation of an equipment authorization, OET and PSHSB will issue an order explaining its reasons as well as how such revocation will be implemented (*e.g.*, halting distribution, marketing, and sales of such equipment, requiring other appropriate actions) and enforced.

*Revocation of existing equipment authorizations on grounds that the equipment is “covered” equipment.* The Commission also concludes that it has the requisite authority under the Communications Act to review any existing equipment authorization that would, under the rules that the Commission adopted in the Report and Order, be “covered” equipment, and to determine the necessity for revoking such authorization, and that the Commission can undertake such revocation pursuant to current rules. The Commission reaches this determination based on the reading of the Commission’s existing authorities. Pursuant to the same authorities discussed above with respect to the equipment authorization program, the Commission has long relied on its authority (modelled along the lines of section 312 of the Communications Act with respect to spectrum licensees) to revoke equipment authorizations under § 2.939(a)(4) “[b]ecause of conditions

coming to the attention of the Commission which would warrant it in refusing to grant an original application.” The Commission concludes that it is well within its responsibilities and mandate, as IPVM has suggested, to revoke an existing equipment authorization under § 2.939(a)(4).

That the Commission has such authority to revoke is confirmed by the Secure Equipment Act. Indeed, as a matter of statutory structure, the Secure Equipment Act can be read as saying two complementary things: one, that the Commission has no discretion with respect to reviewing or approving requests for equipment authorization for equipment listed on the Covered List (as discussed above) after the Report and Order—*i.e.*, the Secure Equipment Act requires that the Commission no longer review or approve them; and two, that the Commission does have discretion (“other than in the rules adopted” here) to exercise its statutory authority to decide whether to take equipment authorization action regarding authorizations granted prior to the Commission’s decision.

First, in sections 2(a)(1) and 2(a)(2), Congress determined that the Commission shall adopt rules that clarify—on a going forward basis—that the Commission will no longer review or approve equipment that is on the Covered List. This is reinforced by Congress’s inclusion of section 2(a)(3)(A), which specifically states that “[i]n the rules adopted under paragraph [2(a)](1),” *i.e.*, the rules the Commission adopted in the Report and Order, “the Commission may not provide for review or revocation of any equipment authorization granted before the date on which such rules are adopted on the basis of the equipment being on the [Covered List].” Read together, sections 2(a)(1), 2(a)(2), and 2(a)(3)(A) state that, with respect to the scope of the Commission’s section 2(a)(2) rules, those rules shall not provide for the review or revocation of existing authorizations. Second, in section 2(a)(3)(B), Congress made clear that the Commission could use its existing authority to adopt non-section 2(a)(2) rules or otherwise examine the necessity of providing for the review or revocation of equipment authorizations granted before any section 2(a)(2) rules—even in cases where the sole basis for the Commission’s equipment authorization action in those circumstances is the equipment being included on the Covered List.

Thus, with regard to the Commission’s discretion under the Secure Equipment Act, with regard to

new equipment authorizations going forward, Congress has taken the discretion out of the Commission’s hands and directed us to stop reviewing or approving applications involving “covered” equipment. Congress has exercised its authority to draw a bright and clear line. As for existing equipment authorizations, Congress has preserved the Commission’s existing authority—and the discretion that comes with the exercise of that authority—to decide whether the Commission should take action based on equipment being added to the Covered List.

Finally, the Commission noted that it’s making no decision in the Report and Order as to whether any particular existing equipment authorization should be revoked. Whether and to what extent and pursuant to what processes the Commission exercises that authority would be based on several considerations, including the public interest and an assessment of the costs and benefits of any such action. As noted above, the procedures for revoking authorizations that would be applicable to authorization(s) granted before adoption of these rules are set forth in § 2.939(b). In the Further Notice of Proposed Rulemaking in this proceeding, the Commission explores streamlining these procedures and seeks comment on other issues relating to revocation.

### C. “Covered” Equipment

In the *NPRM*, the Commission proposed revisions to its equipment authorization rules and procedures under part 2 to prohibit authorization of any “covered” equipment that is identified on the Covered List published by PSHSB. As noted, this Covered List identifies certain equipment that, to date, has been determined—pursuant to the Secure Networks Act—to be communications equipment that poses an unacceptable risk to national security and safety of U.S. persons. Equipment is on the Covered List only if one of four enumerated sources determines such equipment “poses an unacceptable risk to the national security of the United States or the security and safety of United States persons.” As future determinations are made by these four enumerated sources about “covered” equipment, PSHSB will update the Covered List to reflect those determinations.

In the *NPRM*, the Commission proposed and sought comment on how to identify and address particular “covered” equipment that would no longer be permitted to obtain equipment authorizations. Comments on the scope

of what constitutes “covered” equipment vary widely (as discussed in detail below). Several commenters ask for Commission clarification of what constitutes “covered” equipment for the purposes of the instant proceeding. The Commission agrees that sufficient clarity is needed to provide guidance for purposes of administering the prohibition on authorization of “covered” equipment in the Commission’s equipment authorization program pursuant to the part 2 rules. As discussed in the *NPRM*, the Commission’s efforts to revise its equipment authorization program rules to prohibit authorization of “covered” equipment is one of several different efforts by the Commission, as well as various federal agencies, including those pursuant to the Secure Networks Act and section 889 of the 2019 NDAA, to identify and prohibit the use of “covered” equipment that poses an unacceptable risk to national security. Several commenters, including industry associations, express concern that the Commission not take actions in the instant proceeding that would create confusion or conflict with other Commission actions (*e.g.*, the Commission’s Reimbursement Program), and otherwise stress the importance that the Commission work with other federal agencies on these concerns.

Below, the Commission discusses what constitutes “covered” equipment for purposes of the Secure Networks Act, as implemented by the Commission and placed on the Covered List, and the Secure Equipment Act. This includes discussion of the equipment that already has been included on the Covered List to date, specifically “telecommunications equipment” and “video surveillance equipment” produced by five named entities—Huawei, ZTE, Hytera, Hikvision, and Dahua—pursuant to the Secure Networks Act and the determination made by Congress in § 889(f)(3) of the 2019 NDAA. For purposes of implementing the prohibition of the authorization of such equipment in the Commission’s equipment authorization process, the Commission provides guidance on the scope of “covered” equipment. Because the equipment placed on the Covered List is expected to evolve over time based on new determinations concerning equipment made outside of the Commission, the Commission also discusses how any future such determinations will be addressed with respect to prohibiting authorizations of “covered” equipment in the Commission’s equipment authorization program.

# 1. Current “Covered” Equipment on the Covered List

In the *NPRM*, the Commission proposed revisions to its equipment authorization rules and procedures under part 2 to prohibit authorization of any “covered” equipment that is identified on the Covered List published by PSHSB. At the time that the *NPRM* was adopted in June 2021, the only equipment on the Covered List, published pursuant to section 2(c) of the Secure Networks Act, was based on the determination under section 2(c)(3) of that Act, namely Congress’s determination under section 889(f)(3) of the 2019 NDAA concerning equipment produced by five entities—Huawei, ZTE, Hytera, Hikvision, and Dahua (and their respective affiliates and subsidiaries). The Commission notes that, although PSHSB updated the Covered List in March 2022 and in September 2022 to include additional “covered” services and products, the list regarding “covered” equipment has not been updated or otherwise revised. Accordingly, the Commission discusses the “covered” equipment with respect to these same five entities below, the same equipment on the Covered List as discussed in the *NPRM*.

As the Secure Networks Act makes clear, “covered” equipment only includes equipment determined by any of the four enumerated sources to pose an unacceptable risk. The Commission has affirmed this in the instant proceeding as it has in earlier decisions by the Commission. Accordingly, the Commission disagrees with any assertion by commenters that the Commission should prohibit authorization of any equipment that has not been determined to pose an unacceptable risk by the four enumerated sources and placed on the Covered List.

In the *NPRM*, the Commission proposed that OET, with assistance from bureaus across the agency (including PSHSB, WCB, WTB, IB, and EB), develop necessary guidance for use by all interested parties—including applicants and TCBs that help administer the equipment authorization program—as the Commission implements the proposed prohibition on future authorizations of “covered” equipment. The Commission first discusses what, in the first instance, is “covered” equipment on the current Covered List for purposes of the prohibition in the equipment authorization program. The Commission then provides further guidance on the types of equipment that will be included with regard to implementing

and administering the Commission’s prohibition of future authorizations of “covered” equipment under the revised equipment authorization program rules that the Commission adopted in the Report and Order.

“Covered” equipment produced by Huawei and ZTE. As proposed in the *NPRM*, the Commission will prohibit from equipment authorization all equipment produced by Huawei and ZTE (as well as their subsidiaries and affiliates) that is on the Covered List. As identified pursuant to the Secure Networks Act and Congress’s determination under section 889(f)(3) of the 2019 NDAA, such equipment includes both “telecommunications equipment” and “video surveillance equipment” produced by these two entities (and their subsidiaries and affiliates). Specifically, Congress defines “covered telecommunications equipment or services” in section 889(f)(3)(A) as “telecommunications equipment” produced by Huawei and ZTE, and in section 889(f)(3)(C) Congress included “telecommunications or video surveillance services provided” by Huawei or ZTE “or using such equipment (emphasis added).” Combining the equipment identified by Congress in sections 889(f)(3)(A) and (C), the Covered List published by PSHSB states that “covered” equipment under the Secure Networks Act includes “[t]elecommunications equipment” produced or provided by Huawei or ZTE, “including telecommunications or video surveillance services produced or provided by such entity using such equipment.” The Commission was required to place this equipment on the Covered List, and had no discretion not to do so. As the Commission has explained, the Secure Networks Act requires the Commission to accept and incorporate on the Covered List the determinations as provided, and should interested parties seek to reverse or modify the scope of one of these determinations, the party should petition the source of the determination. The Commission further notes that the Congress in the Secure Equipment Act, with its direct reference to this rulemaking, in which the Commission expressly proposed to prohibit authorization of the “telecommunications equipment” and “video surveillance equipment” specified on the Covered List, endorsed inclusion of this equipment on the Covered List as equipment that must not be authorized by the Commission.

In addition, as explained in the *Supply Chain 2nd R&O* and *Supply Chain 3rd R&O*, the Commission need not make any Secure Networks Act

section 2(b)(2) “capability” assessment of the Huawei or ZTE equipment, under either section 2(b)(2)(A) or (B) of the Secure Networks Act, since, in effect, the Commission finds that Congress under section 889(f)(3) of the 2019 NDAA has made that capability determination regarding this equipment, *i.e.*, that it “otherwise pos[es] an unacceptable risk” to national security, pursuant to section 2(b)(2)(C). Thus, for purposes of the prohibition that the Commission is adopting in this proceeding, “covered” equipment includes “telecommunications equipment” and “video surveillance equipment” produced by Huawei and ZTE.

The Commission provided additional guidance and explanation about what equipment constitutes covered “telecommunications equipment” and “video surveillance equipment” for purposes of the prohibition on such equipment authorization.

“Covered” equipment produced by Hytera, Hikvision, and Dahua. The Commission first addresses the various arguments regarding whether “telecommunications equipment” and “video surveillance equipment” produced by Hytera, Hikvision, and Dahua falls within the scope of “covered” equipment under the Secure Networks Act section 2(c)(3) and the determination by Congress under section 889(f)(3)(B) and (C) of the 2019 NDAA concerning those companies’ equipment, and belongs on the Covered List. In its decision, the Commission explains that their “telecommunications equipment” and “video surveillance equipment” was previously determined to be “covered” and has accordingly been placed on the Covered List. The Commission then addresses the extent to which the Commission can, through its equipment authorization program, prohibit authorization of any of the “video surveillance equipment and telecommunications equipment” produced by these companies (or their respective subsidiaries and affiliates). The Commission concludes that it will prohibit in the equipment authorization program authorization of such equipment produced by Hytera, Hikvision, and Dahua “for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes.”

The Commission notes that while this section focuses on the overall scope of what constitutes “covered” equipment on the Covered List, the Commission provides further guidance regarding what types of equipment constitutes “telecommunications equipment” and



“video surveillance equipment” that will be prohibited from obtaining authorization under the Commission’s equipment authorization program.

“Covered” equipment includes certain “video surveillance and telecommunications equipment” produced by Hytera, Hikvision, and Dahua. Hytera, Hikvision, and Dahua each contend that the Secure Networks Act requires that the Commission’s Covered List now remove listing their “video surveillance and telecommunications equipment” as “covered,” and that in any event the Commission should now preclude their equipment from being deemed “covered” and not prohibit authorization of that equipment in the instant proceeding. Following review of the extensive arguments presented by Hytera, Hikvision, and Dahua representatives, the Commission rejects their contentions that the equipment that they produce cannot constitute covered communications equipment under the Secure Networks Act and section 889(f)(3) of the 2019 NDAA, and that it does not belong on the Commission’s Covered List. Accordingly, the Commission rejects arguments by these companies that the Commission now should remove “video surveillance and telecommunications equipment” produced by these entities (or their subsidiaries or affiliates) from the Covered List.

First, in the Secure Networks Act section 2(c)(3) and section 889(f)(3) of the 2019 NDAA, Congress identified as covered communications equipment “video surveillance and telecommunications equipment” produced by these entities (and any of their subsidiaries or affiliates). The Commission notes that in its 2020 decision in the *Supply Chain 2nd R&O*, the Commission already concluded that, pursuant to the Secure Networks Act and its incorporation of section 889(f)(3) of the 2019 NDAA, “telecommunications equipment” and “video surveillance equipment” produced by Hytera, Hikvision, and Dahua is “covered” communications equipment under the Secure Networks Act, and, as a result, PSHSB properly placed this equipment on the Covered List when it first published the list in March 2021. Accordingly, the Commission rejects arguments by these companies that the Commission now should remove inclusion of “video surveillance and telecommunications equipment” produced by these entities (or their subsidiaries or affiliates) from the Covered List.

The Secure Networks Act expressly provides in section 2(c) that the Commission must place on the Covered

List any communications equipment that poses an unacceptable risk to the national security or the security and safety of United States persons “based solely on one or more” of the determinations made by four enumerated sources specified in the Act. Specifically, one of those determinations, set forth in section 2(c)(3) of the Secure Networks Act, provides the following determination relating to communications equipment posing an unacceptable risk: “[t]he communications equipment or service being covered telecommunications equipment or services, as defined in section 889(f)(3)” of the 2019 NDAA. In turn, section 889(f)(3), which was enacted prior to the Secure Networks Act, provides that “[c]overed telecommunications equipment or services” includes “telecommunications equipment” and “video surveillance equipment” produced by Hytera, Hikvision, and Dahua, per section 889(f)(3)(B), as well as “[t]elecommunications or video surveillance services provided by such entities or using such equipment,” per section 889(f)(3)(C) (emphasis added). Given these two subsections of section 889(f)(3), Congress in the Secure Networks Act has identified as “covered” equipment both “telecommunications equipment” and “video surveillance equipment” produced by these entities or used in the provision of video surveillance or telecommunications services; prior to inclusion of section 889(f)(3) in Secure Networks Act section 2(c)(3), this equipment was subject only to the executive branch’s prohibitions of procurement under section 889 of the earlier enacted NDAA because such equipment can pose an unacceptable risk to national security. To remove “telecommunications equipment” and “video surveillance equipment” produced by Hytera, Hikvision, and Dahua from the Covered List, as their representatives request, would ignore Congressional intent regarding its recognition and determination that use of such equipment can pose an unacceptable risk to national security. In the Commission’s view, Congress identified this equipment as posing an unacceptable risk, and the Commission is not in a position to question that or not include it on the Covered List. Furthermore, Congress passed the Secure Equipment Act in response to the instant Commission proceeding and the then-current Covered List, and Congress expressly mandated that the Commission prohibit authorization of equipment on the Covered List as it had

proposed to do in the *NPRM* in this proceeding. Congress therefore intended the prohibition that the Secure Equipment Act requires the Commission to adopt to include the telecommunications equipment and the video surveillance equipment that already was on the Covered List. Given the Commission’s conclusion here that the arguments of Hytera, Hikvision, and Dahua representatives fail on the merits, the Commission need not address Motorola’s contention that their arguments must be denied on the basis of the Hobbs Act.

The Commission disagrees with the assertions that telecommunications and video surveillance equipment produced by Hytera, Hikvision, and Dahua are not “covered” because their respective equipment does not meet the “capability” requirements under section 2(b) of the Secure Networks Act either with respect to being capable of routing or redirecting user data traffic or permitting visibility into any user data or packets or causing the network to be disrupted remotely. As discussed above, the Commission already has concluded in both the *Supply Chain 2nd R&O* and the *Supply Chain 3rd R&O* that the Commission need not make any Secure Networks Act section 2(b)(2) “capability” assessment regarding Hytera, Hikvision, or Dahua equipment, under either section 2(b)(2)(A) or (B) of the Secure Networks Act, since, in effect, Congress under section 889(f)(3) of the 2019 NDAA has made that capability determination pursuant to section 2(b)(2)(C), concluding that video surveillance and telecommunications equipment produced by these entities is “covered” equipment insofar as Congress has determined that it is capable of “otherwise posing an unacceptable risk” to national security. This decision is further supported by the Commission’s discussion of a section 2(b)(2)(C) determination in the *Supply Chain 2nd R&O*. It noted that if an enumerated source in its determination indicates that a specific piece of equipment or service poses an unacceptable risk to the national security of the United States and the security and safety of United States persons, the Commission need not conduct an analysis of the capabilities of the equipment and instead will automatically include this determination on the Covered List. Congress, the enumerated source with regard to determinations about this equipment, has already performed the analysis on whether the equipment—such as video surveillance equipment specifically identified under section

889(f)(3)(B) and (C)—poses an unacceptable risk to the national security of the United States or the security and safety of United States persons as part of its determination. For these reasons as well, the Commission also disagrees with PowerTrunk insofar as it opposes the Commission's adoption of a prohibition on future authorizations of any "covered" equipment that it produces. Regardless of whether PowerTrunk may have been permitted in 2018 for use by certain public safety entities, the issue before us in this proceeding is whether to permit future authorizations of PowerTrunk telecommunications and video surveillance equipment. The Commission rejects the argument that any such PowerTrunk equipment should be exempted from the prohibition that the Commission proposed in the *NPRM*, based on a determination made pursuant to the Secure Networks Act, and that Congress in the Secure Equipment Act directed the Commission to adopt.

In addition, the Commission rejects the arguments that video surveillance equipment is not "covered" under the Secure Networks Act because it is not "communications equipment" or "essential to the provision of advanced communications service," as defined in section 9(4) of the Act. In its *Supply Chain 2nd R&O*, the Commission has already interpreted "communications equipment or service" and what is "essential," codifying that interpretation in § 1.50001(c) of the Commission's rules: "The term 'communications equipment or service' means any equipment or service used in fixed and mobile networks that provides advanced communications service, provided the equipment or service includes or uses electronic components." The Commission also rejects Hikvision USA's further contention that video surveillance equipment is not "used in" fixed and mobile networks, and Hikvision's and Dahua's assertions that such equipment is only "peripheral" equipment and not network equipment and hence not "covered." In identifying such equipment as covered communications equipment under the Secure Networks Act, by reference to section 889(f)(3), Congress intended to capture such video surveillance equipment as "covered" equipment, even if is not core network equipment since the equipment is used (and indeed required) in the provision of a certain type of advanced communications service, *i.e.*, video surveillance services. In addition, the Commission is not persuaded by arguments that because

the video surveillance and telecommunications equipment produced by the entities does not have to be interconnected to a telecommunications or broadband network, it is not "covered" equipment. As acknowledged, Hikvision, Dahua, and Hytera equipment can be interconnected, and often is. The Commission also notes that some of the video surveillance equipment is part of a cloud-based system requiring interconnection.

In sum, "covered" equipment on the Commission's Covered List includes "telecommunications equipment" as well as "video surveillance equipment" produced by Hytera, Hikvision, and Dahua (and their subsidiaries or affiliates), and was properly placed on the Covered List first published by PSHSB in March 2021. The Commission's existing rules rightfully prohibits the use of federal support to purchase or obtain any "covered" equipment on the Covered List, which appropriately includes a prohibition concerning this video surveillance and telecommunications equipment. The Commission also notes that its actions are consistent with the efforts of the Executive Branch in identifying and implementing a prohibition on procurement with respect to certain "covered" video surveillance and telecommunications equipment produced by Hytera, Hikvision, and Dahua.

*Prohibition concerning equipment authorization of "video surveillance and telecommunications equipment" "[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes."* In adopting the prohibition on authorizing "covered" equipment, the Commission is guided by the specific determination set forth in section 889(f)(3)(B) of the 2019 NDAA regarding "covered" "telecommunications equipment" and "video surveillance equipment" produced by Hytera, Hikvision, or Dahua (or their subsidiaries and affiliates). In the *NPRM*, the Commission proposed to prohibit authorizing any "covered" equipment on the Covered List. As discussed in the *NPRM*, pursuant to the Secure Networks Act section 2(c), the Commission must rely solely on the determinations made by the four enumerated sources identified in that section. Section 889(f)(3)(B) by its terms provides that "covered" equipment includes "video surveillance and telecommunications equipment" produced by Hytera, Hikvision, and Dahua "[f]or the purpose of public

safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes." Accordingly, the Commission cannot and will not approve any application for equipment authorization that would allow the marketing and selling of such equipment for those specified uses. At the same time, this determination only includes, as "covered" equipment, video surveillance and telecommunications equipment produced by these entities that is for those particular purposes. Thus, at this time, in the absence of any other of the three identified and specific determinations made by any of the Executive Branch agencies identified in section 2(c) of the Secure Networks Act, the Commission cannot expand "covered" beyond that determination by adopting a blanket or categorical prohibition on authorizing equipment produced by these entities for those other purposes. The Commission's approach regarding this equipment is consistent with the Commission's previous interpretations of section 889(f)(3)(B) in the 2020 *Supply Chain 2nd R&O* and in the language specified in the Covered List, in which the Commission stated that this equipment produced by Hytera, Hikvision, and Dahua (and their subsidiaries and affiliates) is "covered" "to the extent used" for these specified purposes. And, as discussed above, federal agencies in implementing the federal agency procurement prohibitions under section 889 have interpreted this statutory language regarding the scope of "covered" equipment in a like manner.

Accordingly, the Commission is prohibiting authorization to market and sell Hytera, Hikvision, and Dahua "telecommunications equipment" and "video surveillance equipment" (and that produced by their subsidiaries and affiliates) "[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes." For any equipment authorization application for video surveillance and telecommunications equipment produced by these entities, the Commission will impose strict and appropriate conditions on any approved grant, consistent with the Commission's equipment authorization rules. Specifically, the Commission will only conditionally authorize the marketing and sale of such equipment authorization subject to this prohibition. The Commission also will require labeling requirements that prominently state this prohibition. As a condition of

the equipment authorization, the Commission also will impose stringent marketing and sale prohibitions associated with the equipment, which will apply not only with respect to these entities (and their subsidiaries and affiliates), but also to their equipment distributors, dealers, or re-sellers, *i.e.*, every entity down the supply chain that markets or offers the equipment for sale or that markets or sells the equipment to end-users.

Based on the record before us, the Commission is also concerned that adopting conditions alone will not be sufficient to ensure that “covered” equipment is not over time marketed, or ultimately sold, for the purposes prohibited under section 889(f)(3)(B) of the 2019 NDAA. Given that “covered” equipment poses an unacceptable risk if used “[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes,” the Commission adopted additional restrictions as described herein to prevent marketing and sale of Hytera, Hikvision, or Dahua “telecommunications equipment” or “video surveillance equipment” for use for the purpose of public safety, government security, critical infrastructure, or national security.

Based on the record, which highlights the lack of oversight that Hytera, Hikvision, and Dahua have over the marketing, distribution, and sales of their respective equipment in the United States, the Commission is not confident that, absent additional prescriptive measures and Commission oversight, Hytera, Hikvision, and Dahua “telecommunications equipment” or “video surveillance equipment” will not be marketed and sold for those purposes that are prohibited under section 889(f)(3)(B) of the 2019 NDAA. Accordingly, the Commission will require that, before the Commission will permit an equipment authorization of any “telecommunications equipment” or “video surveillance equipment” produced by Hytera, Hikvision, or Dahua (or their subsidiaries or affiliates), these entities must each seek and obtain Commission approval for its respective plan that will ensure that such equipment will not be marketed or sold “[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes.” Any such plan must demonstrate that effective measures are in place that will ensure that equipment distributors, equipment dealers, or others in the supply and distribution chains associated with marketing or sale

of such equipment are aware of this restriction and do not market or sell such equipment to entities for the purposes mentioned above. Such a plan must include well-articulated and appropriate measures at the distributor and dealer levels to ensure that the entity does not market or sell for prohibited purposes. Before any Hytera, Hikvision, or Dahua

“telecommunication equipment” or “video surveillance equipment” will be authorized for market or sale, the applicant seeking approval of any “covered” equipment produced by any of these entities (or their subsidiaries or affiliates) must submit a specific plan associated with the equipment, which will be reviewed by the full Commission and only approved if the measures that are and will be taken are sufficient to prevent the marketing and sale of such equipment for purposes prohibited under section 889(f)(3)(B) of the 2019 NDAA.

The Commission provides guidance on what constitutes “telecommunications equipment” and “video surveillance equipment,” as well as clarifying the scope of the prohibition under section 889(f)(3)(B) concerning “[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes.” Finally, the Commission notes that the actions in this proceeding, including this particular prohibition on authorization of “telecommunications equipment” and “video surveillance equipment” produced by Hytera, Hikvision, and Dahua, are among the several Commission and whole-of-government approaches underway and that are continuing to evolve. As discussed below, as future determinations are made under section 2(c) of the Secure Networks Act regarding “covered” equipment that poses an unacceptable risk to national security, and the Covered List is updated accordingly, authorizations of such equipment will be prohibited as well.

## 2. “Covered” Equipment Produced by Subsidiaries and Affiliates

On the current Covered List, “covered” equipment produced by “subsidiaries and affiliates” of the companies named on the Covered List also are included within the scope of “covered” equipment, and authorization of such equipment will be prohibited as “covered” equipment as a result of the Commission’s revisions to the equipment authorization program rules adopted in this proceeding. Applicants seeking equipment authorizations will

be required to attest (in the form of a written and signed certification) that the equipment for which they are seeking authorizations is not “covered” equipment produced by any of the entities identified on the Covered List, which thus could include equipment produced by the named entities on the Covered List or produced or by any subsidiaries or affiliates of those entities.

**Definitions.** The Commission addresses here the relevant definitions that the Commission will apply in the rules implementing the prohibition on authorization of “covered” equipment to the extent such equipment includes equipment produced by subsidiaries and affiliates of entities specifically named on the Covered List. The Commission starts with “affiliate,” for which it adopted the definition consistent with that adopted by the Commission in its *Supply Chain 2nd R&O*. That order defined “affiliate” as “a person that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another person,” referencing the definition of “affiliate” contained in section 3 of the Communications Act (47 U.S.C. 153(2)). The Commission notes that the definition of affiliate in the Communications Act further states that “[f]or purposes of this paragraph, the term ‘own’ means to own an equity interest (or the equivalent thereof) of more than 10 percent,” and the Commission adopted such further clarification in this proceeding. For purposes of implementation in the Commission’s equipment authorization program, the Commission defines “affiliate” as an entity that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another entity, where the term “own” means to have, possess, or otherwise control an equity interest (or the equivalent thereof) of more than 10 percent.

As for “subsidiary,” the Commission notes generally that a subsidiary is an affiliate that is directly or indirectly controlled by an entity (*e.g.*, corporation) with at least a greater than 50% share. In the context of reviewing foreign ownership under section 310(b) of the Communications Act, the Commission’s rule defines a “subsidiary” of a licensee as “any entity in which a licensee owns or controls, directly and/or indirectly, more than 50 percent of the total voting power of the outstanding voting stock of the entity, where no other individual or entity has de facto control.” The Commission believes that adopting a broader

definition of subsidiary than the one set forth in the Commission's foreign ownership rules is appropriate here in light of the national security purposes of the Secure Equipment Act. For purposes of implementing the prohibition on "covered" equipment, the Commission defines "subsidiary" of an entity named on the Covered List as any entity in which such named entity directly or indirectly (1) holds *de facto* control or (2) owns or controls more than 50% of the total voting power of the entity's outstanding voting stock.

*Names of entities identified on the Covered List that produce "covered" equipment, including subsidiaries and affiliates.* The Commission also adopted a requirement that, to the extent the Covered List identifies named entities as well as certain unnamed associated entities—such as subsidiaries or affiliates—as producing "covered" equipment, each such entity specifically named on the Covered List as producing "covered" equipment must submit information to the Commission regarding that named entity's associated entities. As discussed above, the current Covered List identifies equipment produced by certain named entities and their subsidiaries and affiliates as "covered" equipment. As Motorola notes, the entities on the Covered List do not currently publicly disclose detailed information about their corporate relationships, including the names of their subsidiaries and affiliates, and it contends that it is "imperative" that the Commission have visibility into these relationships. In implementing rules and procedures to prohibit authorization of such "covered" equipment produced by particular entities named on the Covered List and their associated entities (e.g., their respective subsidiaries and affiliates), the Commission finds that it is critical that the Commission, as well as applicants for equipment authorizations, TCBs, and other interested parties, have the requisite, transparent, and readily available information of the particular entities that in fact are such associated entities of the named entities on the Covered List. The Commission finds that having this information on the names of such associated entities promotes effective implementation of and compliance with the prohibition, by providing the Commission and TCBs in advance of reviewing any equipment authorization applications with a list of all those entities to which the Covered List applies. Requiring that this information be provided to the Commission and made public aligns

with the regulatory requirements that the Commission proposed in the *NPRM* and that the Commission has adopted, namely placing responsibilities on applicants to attest that their equipment is not "covered" equipment produced by any of entities identified on the Covered List. This also adds another important informational element to the overall comprehensive regulatory scheme and approach that the Commission is taking to ensure that applications for authorization of "covered" equipment are not submitted to the Commission and that no such equipment authorization is granted. Requiring this information is both reasonable and justified in keeping with the Commission's goal of effectively ensuring that "covered" equipment determined as posing an unacceptable risk to national security under the Secure Networks Act, and prohibited from authorization under the Secure Equipment Act, is not authorized, and helps to ensure that the Commission meet the mandate in the Secure Equipment Act that the Commission not approve grant of any "covered" equipment. Finally, it is also critical that such information be up-to-date and maintained in a place for all interested parties to reference for purposes of compliance with the Commission's rules, including the applicants' attestation requirements.

Accordingly, if "covered" equipment on the Covered List includes equipment produced by named entities as well as associated unnamed entities (e.g., their subsidiaries and affiliates), the Commission will require that each entity specifically named on the Covered List that produces "covered" equipment submit a complete and accurate list to the Commission, within 30 days of effective date of the rules, identifying the names of such associated entities that produce equipment that requires an equipment authorization under the rules the Commission adopted in the Report and Order, and must provide up-to-date information on any changes to the list with respect to any such entities. For each such associated entity (e.g., subsidiary or affiliate), the entity named on the Covered List must provide the following information: full name, mailing address and physical address (if different from the mailing address), email address, and telephone number. If there are changes to a named entity's list of such associated entities, that entity must submit such updated information to the Commission within 30 days of the change(s), and indicate the date on which the particular change(s) occurred.

These submissions must be supported by an affidavit or declaration under penalty of perjury, signed and dated by an authorized officer of the named entity on the Covered List with personal knowledge verifying the truth and accuracy of the information provided about the entity's associated entities. The affidavit or declaration must comply with § 1.16 of the Commission's rules. This information on these entities will be posted on the Commission's website as an appendix to the guidance on "covered" equipment posted by OET and PSHSB, and will be updated with any updated information that the Commission receives. Applicants requesting equipment authorizations will be able to reference this information when making attestations regarding the producer of equipment for which they seek authorizations, as will TCBs, the Commission, and other interested parties.

### 3. Re-Branded ("White Label") Equipment

Particular equipment, including products approved through the Commission's equipment authorization program, may be produced by particular companies or manufacturers and subsequently re-branded by other companies. The Commission notes, for instance, that Dahua USA acknowledges that its video surveillance equipment may be re-branded and sold under re-branded names. IPVM also notes that Hikvision and Dahua video cameras often have been relabeled and sold under another name.

As discussed above, the Commission is prohibiting authorizing "covered" equipment "produced" by any of the named entities (as well as their subsidiaries or affiliates) on the Covered List. Under the prohibition on authorizing equipment "produced" by entities on the Covered List the Commission is also precluding any equipment application by any other entity to the extent that the equipment for which authorization is sought had been produced by entities identified on the Covered List but has been re-branded or re-labeled with other names or associated with other companies. Re-branding of equipment does not change the status of whether the equipment itself is "covered" equipment prohibited from equipment authorization.

### 4. Guidance on Implementing the Prohibition on Authorizing "Covered" Equipment in the Equipment Authorization Program

The Commission affirms its earlier decisions and concludes that, pursuant to the Secure Networks Act and section

889(f)(3) of the 2019 NDAA, “covered” equipment on the current Covered List includes both “telecommunications equipment” and “video surveillance equipment” produced by Huawei and ZTE (and their subsidiaries and affiliates), as well as such equipment produced by Hytera, Hikvision, and Dahua (and their subsidiaries and affiliates) to the extent used “[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes.” Under the rules that the Commission adopted in this proceeding, the Commission will no longer permit the authorization to market or sell any such “covered” equipment in the Commission’s equipment authorization program. As an integral part of the Commission’s implementation of this prohibition, under the Commission’s revised part 2 equipment authorization rules, the Commission will require each applicant for equipment authorization to provide in its application an attestation (in the form of a written and signed certification) that the equipment in its application is not “covered” equipment. Below, the Commission provides additional clarity on what constitutes “covered” equipment that will be prohibited, as several have requested. As a general matter, given the importance of preventing “covered” equipment from being made available for uses that would pose an unacceptable risk to national security or the security of U.S. persons, the terms of determinations made by any of the four enumerated sources and incorporated into the Covered List should be interpreted broadly.

In proposing in the *NPRM* to require applicants for equipment certification to attest that the subject equipment is “not” covered, the Commission recognized the importance of providing guidance to applicants, TCBs, and other interested parties. In particular, the Commission proposed to direct Commission staff (OET, working with PSHSB, WCB, IB, and EB) to develop pre-approval guidance or other guidance to assist in implementing the Commission’s prohibition on authorization of “covered” equipment. Here, the Commission provides guidance to Commission staff as well as applicants, TCBs, and other interested parties regarding the administration and implementation of the prohibition of the authorization of “covered” equipment through the attestation process, the TCBs’ assessment, and the Commission in its implementation and monitoring of the equipment authorization process to

ensure that “covered” equipment is not authorized for marketing or sale.

For purposes of the implementation of the equipment authorization program, the Commission interprets the terms “telecommunications equipment” and “video surveillance equipment” broadly to ensure that equipment that could pose an unacceptable risk is not authorized, in keeping with the Commission’s proposal and its acknowledgement in the Secure Equipment Act of 2021. As discussed below, the Commission delegates to OET and PSHSB, working with other bureaus/offices as appropriate, the authority to provide additional clarity with regard to the scope of covered equipment for purposes of the Commission’s equipment authorization program, to make such information on the Commission’s website, and to revise that information as appropriate. The Commission underscores the importance for each applicant seeking authorization of equipment to exercise due diligence in preparing and submitting its attestation that the subject equipment for which it seeks authorization for market or sale is not “covered.” At the time of the filing of its application for certification of equipment, each applicant must have reviewed the Commission rules and guidance set forth on its web page, and have determined through due diligence that the subject equipment in its application for certification is not “covered.” As discussed above, false statements or representations that the subject equipment is “not” covered will result in denial of an application or revocation of the equipment authorization and potentially additional enforcement action.

As noted in the *NPRM*, the Commission authorizes a wide array of equipment. Under existing rules for certification, such equipment includes base stations, transmitters associated with various licensed services (including mobile phones, land mobile radios), Wi-Fi access points and routers, home cable set-top boxes with Wi-Fi, laptops, intelligent home devices, and various wireless consumer equipment. Equipment that is subject to authorization under existing SDoC procedures includes certain microwave and broadcast transmitters, certain private land mobile equipment, certain equipment for unlicensed use (e.g., business routers, internet routers, firewalls, internet appliances, surveillance cameras, business servers, and certain ISM equipment).

In addition to providing guidance clarifying the nature of “telecommunications equipment” and

“video surveillance equipment,” the Commission also discusses the scope of the prohibition with regard to authorization of Hytera, Hikvision, and Dahua “telecommunications equipment” and “video surveillance equipment.” Pursuant to the determination made by Congress under section 889(f)(3)(B), and as identified on the Covered List, such equipment produced by these entities is “covered” “for purposes of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes.”

*Telecommunications equipment.* Considering the importance of prohibiting authorization of “covered” equipment that poses an unacceptable risk to national security, the Commission interprets “telecommunications equipment” broadly for purposes of the Commission’s equipment authorization program. This approach is consistent with the Commission’s earlier decisions that broadly define “communications equipment” under the Secure Networks Act. It also accords with congressional intent in the Secure Equipment Act of 2021.

In particular, the Commission interprets “telecommunications equipment” as broadly as it previously defined “communications equipment.” Under the approach adopted here, “telecommunications equipment” means any equipment used in fixed or mobile networks that provides advanced communications service, provided the equipment includes or uses electronic components, as defined under § 1.50001(c). Further, taking into consideration the definition of “advanced communications service” under § 1.50001(a), this would encompass any equipment that can be used in such a fixed or mobile broadband network to enable users to originate and receive high quality voice, data, graphics, and video telecommunications using technology with connection speeds of at least 200 kbps in either direction. By taking this broad approach, the Commission brings within the scope of the prohibition a wide range of communications equipment that are used within broadband networks. The Commission’s goal in adopting this definition is to provide clear guidance that promotes regulatory compliance and administrability, as well as regulatory certainty.

The Commission rejects the contention that “telecommunications equipment” under the Secure Networks Act must necessarily exclude all CPE

equipment or IoT equipment, or that “telecommunications equipment” under the Secure Networks Act should be defined in the same manner as the term “telecommunications equipment” is defined under the Communications Act. In interpreting and broadly defining “communications equipment” under the Secure Networks Act, the Commission indicated its concern, consistent with congressional intent, that the Commission protects against the use of insecure equipment in advanced communications services, and it did not indicate an intent to exclude all CPE or IoT equipment from the scope of “covered” equipment under the Act. Nor was there any indication by Congress, when adopting section 889(f)(3) as part of the NDAA of 2019 regarding prohibitions on federal agencies’ procurement of “telecommunications equipment” (or “video surveillance equipment”) that the term “telecommunications equipment” in the NDAA was to be narrowly defined and limited to “telecommunications equipment” as defined in the Communications Act or used by the Commission in certain Commission-focused contexts. As Motorola points out, the NDAA involves a different statutory scheme. As the courts have repeatedly recognized, Congress may have intended to accord different scope to the same language used in different statutes, depending upon the context and purpose of the statutory scheme. Indeed, the Commission notes that the federal agencies’ own procurement rules, whose national security purposes are much more relevant here, define “telecommunications” broadly as “the transmission, emission, or reception of signals, signs, writing, images, sounds, or intelligence of any nature, by cable, satellite, fiber optics, laser, radio, or other electronic, electric, electromagnetic, or acoustically coupled means;” those rules further define “telecommunications services” as meaning “the services acquired, whether by lease or by contract, to meet the Government’s telecommunications needs,” including “the *equipment* necessary to provide such services” (emphasis added). Considering the Commission’s goal of eliminating future authorization of “covered” equipment that poses an unacceptable risk to national security, the Commission does not interpret the scope of “covered” equipment narrowly because a limited view of what constitutes insecure equipment would potentially result in an unacceptable risk to national security and would be inconsistent with the

broader definition used by federal agencies implementing the section 889 prohibition on federal agency procurement of “telecommunications equipment.”

The Commission also notes, for instance, that pursuant to section 5 of the Secure Networks Act, the Commission requires that advanced communications service providers submit annual reports certifying whether they had purchased, leased, rented, or otherwise obtained “covered” equipment after August 18, 2018. The Commission directed the Office of Economics and Analytics (OEA) to administer this data collection, and in doing so it issued guidance (“Supply Chain Annual Reporting 2022 Filing Instructions”) to define the information that advanced service providers were required to file and to act as a guide to assist filers with submitting the necessary information. Pursuant to these instructions, advanced service providers are required to submit information on “covered” equipment that is in different layers of their networks, including in the “access layer,” the “distribution layer,” and the “core layer.” “Access layer” equipment is equipment associated with providing and controlling end-user access to the network over the “last mile,” “local loop,” or “to the home” (e.g., optical terminal line equipment, optical distribution network devices, customer premises equipment (to the extent owned by the advanced services provider), coaxial media converters, wavelength-division multiplexing (WDM) and optical transporting networking (OTN) equipment, and wireless local area network (WLAN) equipment). “Distribution equipment” includes middle mile, backhaul, and radio area network (RAN) equipment (e.g., routers, switches, network security equipment, WDM and OTN equipment, and small cells). “Core layer” equipment is associated with the backbone infrastructure (e.g., optical networking equipment, WDM and OTN, microwave equipment, antennas, RAN core, Cloud core, fiber, and data transmission equipment). The Commission affirms the broad approach taken by OEA in implementing the annual reporting requirement on “covered” equipment—including its specific inclusion of “access layer,” “distribution layer,” and “core layer” equipment in networks providing advanced communications services as falling within the scope of what constitutes “covered” equipment under the Secure Networks Act.

Because of the wide array and variety of devices in the marketplace, the

Commission cannot in this document identify all of the categories or types of equipment that would constitute “telecommunications equipment.” The Commission nonetheless proffers some additional clarity consistent with the broad definition of “telecommunications equipment” for purposes of implementing the prohibition on authorization of “covered” equipment in this proceeding.

Huawei and ZTE each produce, among other things, different types of equipment that requires certification, including base stations, cell phone and smart phone handsets, tablets, and routers that operate under particular rules for licensed services (e.g., part 22, 24, 27, 90, 96) as well as various unlicensed devices, including Wi-Fi routers. Hytera produces, among other things, base station units and repeaters, as well as trunking systems PLMR/DLMR handsets and two-way radios, which operate under various rules for licensed services (e.g., part 22, 24, 80, 90, 95). Hytera representatives assert not only that Hytera equipment is not “covered” because it is “peripheral” equipment or CPE, but also contend generally that Hytera equipment is not “telecommunications equipment” or “covered communications equipment” because it is generally not interconnected to a fixed or mobile broadband network (although its notes that a small subset of handsets (e.g., PowerTrunk TETRA) is so designed). As noted above, Hikvision and Dahua representatives also each generally assert the company does not produce any “telecommunications equipment,” and argue that no CPE and IoT can be deemed such equipment. Hikvision USA further asserts that, while Hikvision does produce U-NII router equipment for unlicensed use, such equipment is not “covered” because it is CPE and is within an end-user’s internal enterprise network on the user’s side of the gateway router and therefore not broadband equipment.

Whether particular equipment is covered telecommunications equipment will turn on applying the Commission’s interpretation of what constitutes such equipment. As discussed, the Commission believes that Congress intended to take a broad view of what constitutes “covered” “telecommunications equipment” for purposes of the prohibition on future equipment authorizations. Accordingly, the Commission concludes not only that the types of “telecommunications equipment” specifically identified in the Supply Chain Annual Reporting 2022 Filing Instructions are “covered”

for the purposes of this proceeding, including equipment such as cellular base stations, backhaul, and core network equipment, but the Commission also clarifies that handsets designed for operation over fixed or mobile networks providing advanced communications services also are “covered.” The Commission makes this decision recognizing that handsets generally, as well as many CPE and IoT devices, meet the broad definition the Commission adopted insofar as these devices incorporate electronic components, could enable users to originate and receive high quality voice, data, graphics, and video telecommunications with connection speeds of at least 200 kbps in either direction, and may be the end points of most broadband networks which makes them part of the network. The Commission disagrees with Hikvision USA’s suggestion that the Commission has already concluded in the *Supply Chain 3rd R&O* that handsets, CPE, and IoT necessarily are not “covered” equipment when it observed that handsets and other CPE including IoT used by end users are different from cell sites, backhaul and core network equipment and then declined to require that such equipment be removed, replaced, and reimbursed under the Reimbursement Program. That observation only addressed what equipment would be eligible for reimbursement under the Reimbursement Program, and was not intended to define the nature of what equipment should be considered “covered.” As Motorola rightly notes, and as the Commission point about above, that proceeding limited the scope of the Reimbursement Program to a subset of the Covered List, and the equipment and services on the Covered List was not at issue. In the Commission’s equipment authorization program, the Commission is not concerned with the Reimbursement Program but instead is focused on preventing future authorization of equipment that could pose an unacceptable risk to national security or the security and safety of U.S. persons. The Commission concludes that handset equipment designed for operation over broadband networks and that enable users to originate and receive high quality voice, data, graphics, and video telecommunications with connection speeds of at least 200 kbps in either direction fall within the broad scope of the Commission’s interpretation of “telecommunications equipment” and is “covered.” Accordingly, the Commission notes that Huawei and ZTE

handsets, and Hytera handsets to the extent designed to operate over broadband networks, are “covered.” The Commission also notes that this approach fully accords with congressional intent in the Secure Equipment Act, in which Congress sought to ensure that the Commission not approve devices that pose a national security risk and that equipment for which public funding was prohibited because it poses an unacceptable risk also should be addressed in the equipment authorization program. As for other CPE or IoT devices, whether particular equipment is “covered” will depend on whether it meets the requirements for “covered” equipment discussed above. These terms have been defined by industry in a variety of ways and contexts, and could include a wide range of equipment and technologies that may connect to the internet or other broadband networks without any specific regard as to whether the equipment would meet the requirements of “covered” telecommunications equipment under the Secure Networks Act as interpreted by the Commission (e.g., enable users to originate high quality voice, data, graphics, and video telecommunications with connection speeds of at least 200 kbps in either direction).

Because the Commission authorizes a wide range of equipment, and because additional clarification on “covered” equipment may be needed, the Commission delegates to OET and PSHSB, working with WTB, IB, WCB, EB, and OGC, as appropriate, to develop and finalize additional clarifications as needed to inform applicants for equipment authorization, TCBs, and other interested parties with more specificity and detail on the categories, types, and characteristics of equipment that constitutes “telecommunications equipment” for purposes of the prohibition on future authorization of “covered” equipment identified on the Covered List. As the Commission notes above, federal agencies are actively engaged in prohibiting procurement of “covered” equipment, including “telecommunications equipment” as defined by section 889(f)(3) of the 2019 NDAA. As OET and PSHSB develop more detailed guidance for purposes of the prohibition in the equipment authorization program, they may also review efforts from other federal agencies, such as the General Services Administration’s efforts in its implementation of the procurement prohibition and the types of “telecommunications equipment” that constitute such “covered” equipment,

the Federal Acquisition Security Council, the Department of Homeland Security’s Information and Communications Supply Chain Risk Management Task Force, or other federal efforts, if those efforts are relevant to development of the guidance.

The Commission further directs OET and PSHSB to issue future clarifications in a Public Notice, and to post these clarifications on the Commission’s website for ready access by all interested parties. This guidance will serve as a reference for applicants and other stakeholders to provide consistency and clarity for purposes of complying with the Commission’s rules prohibiting authorization of “covered” equipment. OET and PSHSB are further directed to provide updated clarifications as appropriate, which could be further informed by information provided by interested parties. The Commission is also requiring that a Public Notice be issued with any updates to the guidance, along with an updated website. This guidance also can be used to assist TCBs in their assessments of equipment authorization applications to help preclude authorization of any “covered” equipment.

*Video surveillance equipment.* As with “telecommunications equipment,” considering the importance of prohibiting authorization of “covered” equipment that poses an unacceptable risk to national security, the Commission broadly interprets “video surveillance equipment” under the Secure Networks Act and section 889(f)(3) of the 2019 NDAA for purposes of the Commission’s equipment authorization program. As discussed above, taking a broad approach to defining “covered” equipment also is consistent with the Commission’s earlier decisions defining “covered” equipment broadly under the Secure Networks Act, and is in accord with congressional intent set forth in the Secure Equipment Act.

In particular, the Commission interprets “video surveillance equipment” consistent with the definition in the Commission’s rules concerning “communications equipment” under the Secure Networks Act, to include any equipment that is used in fixed and mobile networks that provides advanced communications service in the form of a video surveillance service, provided the equipment includes or uses electronic components. In keeping with the definition of “advanced communications service,” the Commission intends with this definition



to encompass all equipment that is designed and capable for use for purposes of enabling users to originate and receive high-quality video telecommunications service using any technology with connection speeds of at least 200 kbps in either direction.

As discussed, Hikvision and Dahua each produce a wide range of products that are associated with video surveillance capabilities, including cameras, video recorders, and network storage devices. Although Hytera asserts that it does not produce any video surveillance equipment, the Commission notes that, among other things, it manufactures “body-worn camera” equipment. In their submissions, Hikvision and Dahua representatives each contend that its video surveillance equipment is “peripheral” or CPE, and hence not “covered.” The Commission rejects that view altogether, particularly given that section 889(f)(3) specifically discusses “video surveillance equipment” as “covered,” which reflects Congress’s clear intent that video surveillance equipment can pose an unacceptable risk to national security. Hikvision and Dahua representatives also contend their respective video surveillance equipment is not “covered” because the equipment does not require connection to the internet (an end user’s choice); Hikvision USA does acknowledge, however, that some of its video surveillance equipment (HikConnect) does require internet connection, and that in any event its equipment poses no danger because it is secure. Dahua USA contends, among other things, that its digital video recorders, network video recorders, data storage devices, and video surveillance servers should not be deemed “covered.” IPVM asserts that most video surveillance equipment today has internet connectivity as a widely-demanded feature, and notes in particular that Hikvision surveillance cameras are generally marketed as internet-protocol (IP) cameras that are designed and marketed for use connected to internet. IPVM also disagrees with Dahua USA’s contention that video recorders are not “covered” as “video surveillance equipment,” and generally contends broadly that Hikvision and Dahua equipment poses a threat to the American public. Given the concerns Congress raised about the potential risks to national security associated with such video surveillance capabilities, the Commission believes it intended to take the broad view on what constitutes video surveillance equipment, and concludes that it includes not only surveillance cameras,

but also video surveillance equipment associated with video surveillance services that make use of broadband capabilities, such as video recorders, video surveillance servers, and video surveillance data storage devices. The Commission makes this determination recognizing that these devices are capable of storing and sharing their content over broadband networks and thus being connect to the network, they become part of the network. The Commission also concludes that Hytera equipment that includes capabilities associate with video surveillance service, such as “body cams,” which are generally designed to connect to the internet, also is “video surveillance equipment” that is “covered.”

As with “telecommunications equipment,” the Commission delegates to OET and PSHSB, working with WTB, IB, WCB, EB, and OGC, as appropriate, to develop and finalize additional guidance to inform applicants for equipment authorization, TCBs, and other interested parties in more specificity and detail, information on the categories, types, and characteristics of equipment that constitutes “video surveillance equipment.” As OET and PSHSB develop further clarification, the Commission authorizes them also to review efforts from other federal agencies, such as the General Services Administration’s efforts in its implementation of the procurement prohibition and the types of “video surveillance equipment” that constitute such “covered” equipment under section 889(f)(3), the Federal Acquisition Security Council, the Department of Homeland Security’s Information and Communications Supply Chain Risk Management Task Force, or other federal efforts, if those efforts are relevant to development of further clarification on what constitutes “covered” equipment.

*For the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes.* Pursuant to the Secure Networks Act and section 889(f)(3)(B) of the NDAA of 2019, the Commission is prohibiting, as “covered” equipment, the authorization of any “telecommunications equipment” or “video surveillance equipment” produced by Hytera, Hikvision, and Dahua (or their subsidiaries and affiliates) “[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes.” As with “telecommunications equipment” and “video surveillance

equipment,” the Commission interprets the scope of this section 889(f)(3)(B) prohibition broadly given the importance of preventing “covered” equipment from being made available for prohibited uses that would pose an unacceptable risk to national security or the security of U.S. persons.

In particular, the Commission construes the scope of elements associated with these purposes—public safety, government facilities, critical infrastructure, and national security—broadly with respect to the implementation in the Commission’s equipment authorization program of the prohibition concerning “covered” Hytera, Hikvision, and Dahua equipment pursuant to the Secure Networks Act and section 889(f)(3)(B) of the 2019 NDAA. The Commission interprets the phrase “[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes” broadly, *i.e.*, as having broad scope with respect to any prohibition relating to covered communications equipment. Terms comprising this phrase—public safety, government facilities, critical infrastructure, and national security—are each construed broadly in order to prohibit authorization of equipment that poses an unacceptable risk to national security of the United States or to the security or safety of U.S. persons. The Commission discusses each of these terms below, and how the Commission broadly construes them consistent with the Secure Networks Act, section 889(f)(B) of the NDAA, and the Commission’s goals in this proceeding to protect national security and the security and safety of U.S. persons.

With respect to “public safety,” the Commission finds that this includes services provided by state or local government entities, or services by non-governmental agencies authorized by a governmental entity if their primary mission is the provision of services, that protect the safety of life, health, and property, including but not limited to police, fire, and emergency medical services. For purposes of implementing the Secure Networks Act and the Secure Equipment Act, the Commission interprets public safety broadly to encompass the services provided by federal law enforcement and professional security services, where the primary mission is the provision of services, that protect the safety of life, health, and property. The Commission believes that this best fulfills Congress’ intent with respect to the scope of public safety as that term is used in section 889(f)(3) in connection with

“covered” Hytera, Hikvision, and Dahua equipment and the other terms in that section.

With respect to the term “government facilities,” the Commission finds instructive the Cybersecurity and Infrastructure Security Agency’s (CISA) view of what constitutes the government facilities sector. According to CISA, the government facilities sector includes “a wide variety of buildings, located in the United States and overseas, that are owned or leased by federal, state, local, and tribal governments.” In addition to facilities that are open to the public, CISA notes that others “are not open to the public [and] contain highly sensitive information, materials, processes, and equipment,” and that these facilities include and are not limited to “general-use office buildings and special-use military installations, embassies, courthouses, national laboratories, and structures that may house critical equipment, systems, networks, and functions.” CISA also notes that “[i]n addition to physical structures, the sector includes cyber elements that contribute to the protection of sector assets (e.g., access control systems and closed-circuit television systems) as well as individuals who perform essential functions or possess tactical, operational, or strategic knowledge.” The Commission believes that this description provides ample guidance for purposes of what constitutes “government facilities” for implementation of the prohibition that the Commission adopts in this proceeding.

With regard to scope of “critical infrastructure” and the prohibition that the Commission is adopting in this proceeding, the Commission applies the meaning provided in section 1016(e) of the USA Patriot Act of 2001, namely, “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” Presidential Policy Directive 21 (PPD–21) identifies sixteen critical infrastructure sectors: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, health care and public health, information technology, nuclear reactors/materials/waste, transportation systems, and water/waste water systems. In this connection, CISA, through the National Risk Management Center (NRMCC), published a set of 55 National Critical

Functions (NCFs) to guide national risk management efforts. The CISA/NRMCC guide defines “critical infrastructure” similar to how that term is defined in the USA Patriot Act. Specifically, it defines the NCFs as “functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.” For purposes of implementing the rules the Commission adopted, the Commission finds that any systems or assets, physical or virtual, connected to the sixteen critical infrastructure sectors identified in PPD–21 or the 55 NCFs identified in CISA/NRMCC could reasonably be considered “critical infrastructure.”

As for “national security,” for purposes of this proceeding, the Commission interprets this term broadly as encompassing a variety of high-profile assets involving government, commercial, and military assets. In this connection, the Commission notes that section 709(6) of the Intelligence Authorization Act for Fiscal Year 2001, provides that “‘national security’ means the national defense or foreign relations of the United States.” Accordingly, the Commission will rely on this definition for guidance.

The Commission delegates to OET and PSHSB, working with WTB, IB, WCB, EB, and OGC, as appropriate, to develop further clarifications to inform applicants for equipment authorization, TCBs, and other interested parties with more specificity and detail. As the Commission develops more detailed guidance, the Commission authorizes OET and PSHSB also to review efforts from and coordinate as necessary with the Commission’s federal partners, such as but not limited to the Department of Justice, Department of Commerce, Department of Homeland Security, and Federal Bureau of Investigation.

**Declaratory ruling.** To the extent an interested party may seek to clarify whether particular equipment is “covered” for purposes of the equipment authorization prohibition, it can bring a request for declaratory ruling before the Commission. The Commission, in its 2020 *Supply Chain 2nd R&O*, similarly noted that any interested party that may seek to clarify whether a specific piece of equipment is included as “covered” on the Covered List could seek a declaratory ruling. At the same time, the Commission notes again that it has no discretion to reverse or modify determinations from the four enumerated sources under the Secure Networks Act that are responsible for

those determinations, which the Commission must accept and include on the Covered List as provided, and that should a party seek to reverse or modify any such determination, it should petition the source of the determination. Moreover, the seeking of clarification by any party does not entitle such party to any presumption, nor is it the basis for arguing, that specific equipment is not “covered,” absent additional clarification from the Commission. The Commission delegates to OET and PSHSB authority to issue such declaratory rulings consistent with principle of broad interpretation of terms given the importance of preventing “covered” equipment from being made available for prohibited uses that would pose an unacceptable risk to national security or the security of U.S. persons, as illustrated above.

#### 5. Future Updates on “Covered” Equipment and the Covered List

As noted, the Commission anticipates that the Covered List, which was most recently updated and published on September 20, 2022, will continue to be revised in the future based on further determinations about communications equipment made by any one of the four enumerated sources that are identified in section 2(c) of the Secure Networks Act. As discussed above, to date, the only determination that specifically concerns communications equipment is that made under section 2(c)(3) of the Secure Networks Act, specifically the determination made by Congress in section 889(f) of the 2019 NDAA. Future determinations concerning communications equipment could involve determinations by any of the other three enumerated sources as specified under the Secure Networks Act—per section 2(c)(1), “[a] specific determination made by any executive branch interagency body with appropriate national security expertise, per including the Federal Acquisition Security Council established under section 1322(a) of title 41, United States Code; per section 2(c)(2), “[a] specific determination made by the Department of Commerce pursuant to Executive Order No. 13873 (84 FR 22689; relating to securing the information and communications technology and services supply chain)”; and per section 2(c)(4), “[a] specific determination made by an appropriate national security agency.”

As noted above, the Commission is required to monitor the status of determinations in order to update the Covered List by modifying, adding, or removing “covered” equipment on the Covered List, pursuant to § 1.50003.

Under the rules adopted in the Report and Order, the Commission will no longer authorize for marketing or sale equipment that has been placed on the Covered List, as that list evolves.

The Commission guidance provided in this document, along with the delegation of authority directing OET and PSHSB to publish and maintain information on the Commission's website concerning "covered" equipment should serve to enable implementation of updates concerning equipment that are placed on the Covered List. The Commission notes, for instance, that a new determination might modify the "covered" equipment on the Covered List only with regard to adding or removing the named entities that produce equipment that poses an unacceptable risk to national security. If so, then the guidance on the Commission's website can readily be updated on delegated authority and the added equipment will be prohibited in the Commission's equipment authorization program. The Commission recognizes, however, that a future determination by one of the four enumerated sources that results in an updated Covered List with respect to new types of equipment that pose an unacceptable risk potentially could require further consideration on delegated authority, consistent with the approach discussed above; if so, the Commission directs OET and PSHSB to so indicate through Public Notice, including discussion of the process by which the guidance will be developed and provided.

#### D. Other Issues

##### 1. Cost-Effectiveness and Economic Impact

In the *NPRM*, the Commission stated that its proposed revisions to the Commission's equipment authorization rules and processes to prohibit authorization of "covered" equipment that had been determined by any one of the four enumerated source outside of the Commission as posing an unacceptable risk to national security would not be subject to a conventional cost-benefit analysis. The Commission stated that because it has no discretion to ignore these determinations, a conventional cost-benefit analysis—which would seek to determine whether the costs of the proposed actions would exceed the benefits—is not directly called for. Instead, the Commission stated that it would consider whether its actions would be "a cost effective" means to prevent this dangerous equipment from being introduced into the Commission's nation's

communications networks, and sought comment on the Commission's proposed revisions to the equipment authorization rules and procedures.

The Commission recognizes that adopting a prohibition on the authorization of "covered" equipment may result in economic impacts on entities directly or indirectly associated with the "covered" equipment identified on the Covered List. However, as the Commission notes above, the rules adopted in the Report and Order regarding future authorizations of "covered" equipment are mandated by the Secure Equipment Act, requiring that the Commission will not approve any application for equipment authorization for equipment that is on the Covered List. The equipment included on the Covered List was determined by other expert agencies as posing an unacceptable risk to national security. As noted in the *NPRM*, because the Commission has no discretion to ignore the congressional mandates and other expert agencies' determinations, the Commission finds that a full cost-benefit analysis is not required with respect to the actions that the Commission is taking in this proceeding. Moreover, as the Commission explains below, it finds that the rules that the Commission adopted are a cost-effective approach to carry out the requirements of the Secure Equipment Act.

*Certification rules and procedures.* The Commission finds that the revision of § 2.911 requiring that applicants for equipment authorizations in the certification process attest that their equipment is not "covered" equipment on the Covered List while also indicating whether they are any entity identified on the Covered List, coupled with procedures for revocation for false statements or representations made in the application for certification, is a reasonable and cost-effective method to ensure that "covered" equipment is not certified. Because the attestation requirement is general, rather than a specific provision that directly relates to the equipment identified on the current Covered List, the Commission believes that most applicants will rely on boilerplate language that, once incorporated for a single certification, will be of negligible cost for an applicant to include in future applications. The Commission expects that the procedures for revocation for false statements or misrepresentations will deter most applicants from false attestations because of the cost that revocation would impose on an applicant. Moreover, the Commission notes that the attestation requirement

that the Commission is adopting is more cost effective than an alternative approach, such as a verification process whereby a third party would confirm that equipment being certified is not on the Covered List; that type of third party verification would be substantially more costly to applicants and would likely slow innovation. The Commission believes that the costs it's imposing are reasonable in light of the national security goals.

Similarly, the Commission finds that requiring that each applicant for equipment certification designate a contact in the United States to act as an agent for service of process is reasonable and cost effective. No commenters raised concerns about the cost-effectiveness of this approach. As discussed above, the Commission has encountered difficulties in achieving service of process for enforcement matters involving foreign-based equipment manufacturers, and this helps ensure that the attestation requirement and other requirements associated with the prohibitions on "covered" equipment are enforceable.

*SDoC rules.* In light of the Commission's limited direct involvement in the SDoC process, the Commission finds that the rule prohibiting any of the entities (or their respective subsidiaries or affiliates) specified on the Covered List from using the SDoC process to authorize any equipment is a reasonable, cost-effective approach to safeguard national security. Because these entities or their subsidiaries or affiliates may produce "covered" equipment that poses an unacceptable risk to national security, even if these entities provide assurance that their equipment not included on the Covered List complies with appropriate technical standards, the Commission cannot be confident that such equipment does not pose a risk to national security. Directing all equipment authorization applications produced by entities named on the Covered List through the certification process, coupled with the Commission's revisions to the SDoC attestation requirements, will allow appropriate scrutiny and oversight by the Commission to ensure consistent application of the Commission's prohibition on further equipment authorization of "covered" equipment.

The Commission also concludes that adopting, as proposed, the requirement that all responsible parties seeking to utilize the SDoC process attest that the subject equipment is not produced by any entities (or their respective subsidiaries or affiliates) identified on the Covered List is a reasonable and

cost-effective means of ensuring that any equipment produced by those entities, instead is processed through the equipment certification process. The Commission finds this attestation requirement provides an appropriate means to ensuring that the SDoC process cannot be used to evade the Commission's restriction on use of the SDoC process (and instead require certification) with regard to entities that produce "covered" equipment.

The adopted rules associated with the SDoC process are narrowly tailored and a cost-effective means of achieving the Commission's overarching national security goals in this proceeding. They also are more cost-effective than other alternatives, such as changing the general rules by, for instance, requiring a registry or a central database specific to entities on the Covered List or setting up a novel verification process for such entities. The Commission's existing certification rules and procedures already encompass such means of verification without creating the need to design a new system to mitigate national security risk. Because the Commission's prohibition applies to subsidiaries and affiliates, when combined with the attestation requirement for responsible parties it will incentivize domestic importers who serve as responsible parties to take the straightforward steps to ensure that equipment produced by entities that produce "covered" equipment are processed in a consistent fashion pursuant to the certification process. This will substantially reduce the cost of enforcing the Commission's prohibition on importation and marketing of equipment on the Covered List.

## 2. Constitutional Claims

The Commission is unpersuaded by certain constitutional objections raised by Huawei Cos., Hikvision USA, and Dahua USA. Consequently, these arguments provide no basis for undercutting the Commission's decision to adopt new equipment authorization rules in the Report and Order.

### a. Bill of Attainder

The Commission rejects the claims of Huawei Cos., Hikvision USA, and Dahua USA that denying equipment authorizations for equipment on the Covered List would represent an unconstitutional bill of attainder. The Supreme Court has identified three elements of an unconstitutional bill of attainder: (1) "specification of the affected persons," (2) "punishment," and (3) "lack of a judicial trial." The Commission finds the showings in the

record regarding the first and second elements inadequate here.

As a threshold matter, the Commission clarifies the framing of the Commission's bill of attainder analysis in light of the different formulations of those arguments employed by commenters. Depending in part on whether commenters raised their bill of attainder concerns before or after the enactment of the Secure Equipment Act, those arguments focused variously on: section 889 of the 2019 NDAA (which provided one of the four triggers for inclusion on the Covered List under the Secure Networks Act); the Secure Equipment Act (which directed the Commission to enact rules clarifying that it would not issue equipment authorizations for equipment on the Covered List published by the Commission under the Secure Networks Act); or the new Commission rules themselves.

Because it is the Secure Equipment Act that ultimately directs the Commission to enact rules yielding the results that are the focus of commenters' bill of attainder concerns, the Commission frames the bill of attainder analysis in terms of that statute. Nonetheless, the Commission makes clear that the analysis below provides sufficient grounds to reject commenters' bill of attainder arguments however they are framed or viewed.

The Commission rejects claims that the Secure Equipment Act is an unconstitutional bill of attainder for a number of independent reasons. For one, it is not clear that the constitutional prohibition on bills of attainder protects corporations, as opposed to individuals. To the extent that it does not protect corporations, its protections would be unavailable to the commenters that raised bill of attainder concerns here. Even if the constitutional prohibition on bills of attainder does protect corporations, however, courts have recognized that "it is obvious that there are differences between a corporation and an individual under the law," and as a result "any analogy between prior [bill of attainder] cases that have involved individuals and [cases] involv[ing] a corporation, must necessarily take into account this difference." At a minimum, then, the distinction between corporations and individuals informs the Commission's analysis below.

*The "specification" criteria.* In significant part, the Secure Equipment Act also does not involve a specification of the affected persons as necessary to constitute a bill of attainder. Although initial iterations of the Covered List—identifying the equipment, products,

and services of certain specified companies—had been published by the time the Secure Equipment Act was enacted, the Covered List required by the Secure Networks Act was designed to evolve over time, expanding or contracting based on the four statutory triggers for inclusion on that list. Thus, the Commission is not persuaded that the specificity prong would be satisfied by the existence of the Covered List at the time of the Secure Equipment Act's enactment.

Nor do most of the Secure Networks Act's triggers for inclusion on the Covered List represent a "specification" of affected persons for bill of attainder purposes. The first, second, and fourth triggers under the Secure Networks Act each turn on future "specific determination[s]" by relevant executive agencies and neither specifically identify companies or individuals by name, nor rely on a framework where the potentially-covered class ultimately subject to inclusion on the Covered List could be easily identified at the time the Secure Equipment Act was enacted. Nor do those triggers turn on past conduct defining the affected individual or group in terms of "irrevocable acts committed by them." Consequently, the Commission concludes that those triggers do not satisfy the "specification" prong of the bill of attainder analysis. Admittedly, aspects of the trigger based on section 889(f)(3) of the 2019 NDAA do rely on certain classes of products and services from specifically-identified companies. But the Secure Network Act's triggers do not otherwise identify the entities or individuals with products or services potentially subject to inclusion on the Covered List by name or in a manner that would render the covered class easily ascertainable when the Secure Equipment Act was enacted.

Aspects of the section 889-based trigger also do not appear to satisfy the "specification" criteria. For example, in addition to applying to certain classes of equipment and services from specifically-identified companies, section 889(f)(3) of the 2019 NDAA also covers "[t]elecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country." Whatever individual companies might know or suspect about themselves, the Commission is not persuaded that the

class of companies potentially covered by that criteria would have been easily ascertainable to Congress at the time of the Secure Equipment Act's enactment. Nor is the Commission persuaded that ownership by, or connection with, the Chinese government, even if existing at a given point in time, are irrevocable acts that could not be altered in the future thereby affecting whether given companies were potentially implicated by that trigger.

*The "punishment" criteria.* Even to the extent that the Secure Equipment Act meets the "specification" prong, the Commission is not persuaded that the denial of equipment certification represents a "punishment" under bill of attainder clause precedent. A "punishment," in this context, is not merely a burden. To determine whether a statute imposes punishment for purposes of the bill of attainder clause, courts look to: "(1) whether the challenged statute falls within the historical meaning of legislative punishment; (2) whether the statute, viewed in terms of the type and severity of burdens imposed, reasonably can be said to further nonpunitive legislative purposes; and (3) whether the legislative record evinces a congressional intent to punish." While courts weigh these factors together, "the second factor—the so-called 'functional test'—invariably appears to be the most important." Even where a statute imposes a sanction falling within the historical meaning of punishment under the first factor, it is not a bill of attainder if it "reasonably can be said to further nonpunitive legislative purposes" under the second factor and the legislative record does not contain "'smoking gun' evidence of punitive intent" under the third.

The party challenging a statute on attainder grounds bears the burden to "establish that the legislature's action constituted punishment and not merely the legitimate regulation of conduct." And because statutes are "presumed constitutional," "only the clearest proof [will] suffice" to invalidate a statute as a bill of attainder. The record here falls far short of the required showing.

With respect to the historical test regarding punishment, Hikvision USA and Dahua USA contend that denial of equipment authorization for equipment on the Covered List resembles "an employment bar, banishment, and a badge of infamy." The Commission finds these comparisons unpersuasive. For one, "[b]ecause human beings and corporate entities are so dissimilar," any analogy between the acts at issue in the employment bar cases and the restriction on equipment authorization under the Secure Equipment Act is

"strained at best." That distinction is important given the rationales underlying prior employment bar decisions. The Supreme Court extended "punishment" to include employment bars, in part, because the restrictions at issue "violated the fundamental guarantees of political and religious freedom." The record does not reveal such concerns here.

While there is some retrospective aspect of section 889—namely, that there needed to be a basis to create the terms of the statute—that is common. Generally, all statutes have prospective and retrospective bases. But the focus of punishment in the bill of attainder context is a determination of past wrongdoing and sanctioning that conduct. That is what is missing from section 889 and that is what distinguishes section 889 from functionally appearing punitive. Thus, the fact that section 889 does not serve as a trial-like adjudication with a retrospective focus supports the Government's assertion that section 889 is a nonpunitive statute. But the analysis does not end here."

Rather than representing something akin to an employment bar, the Commission finds the limitations much more analogous to line-of-business restrictions, which precedent commonly does not treat as imposing a punishment. Companies with equipment on the covered list remain free to manufacture, import, and market equipment that does not require equipment authorization from the Commission, for example, and the Secure Equipment Act also does not prohibit companies' business activities not involving the United States. Thus, unlike the statutes at issue in the employment bar cases, the Secure Equipment Act does not prevent companies with equipment on the Covered List from engaging in their chosen businesses in those respects.

The Commission also rejects claims that the limitations on Commission-issued equipment authorizations resemble banishment, or exile, is the "[c]ompelled removal or banishment from one's native country." It has "traditionally been associated with deprivation of citizenship, and does more than merely restrict one's freedom to go or remain where others have the right to be: it often works a destruction of one's social, cultural, and political existence." Claims of banishment therefore typically arise in cases involving denaturalization, denationalization, and deportation proceedings. In light of this context, it is questionable whether banishment applies to corporations at all.

Alternatively, even if banishment does apply to corporations, the Secure Equipment Act does not "banish" from the United States those companies with equipment on the Covered List. The statute does not destroy those companies' social, cultural, or political existence in this country. And it does not remove those companies from the United States (or any subdivision thereof), nor does it restrict their ability to manufacture, import, and market equipment in the United States that is not included on the Covered List.

The distinction between corporations and individuals also is important because "the stain of a brand of infamy or disloyalty," characteristic of bills of attainder, matters to individuals in a way that it does not to corporations. Unlike "flesh-and-blood humans . . . who, most likely, have but one country of citizenship," as well as "neighbors and colleagues and communities in whose good graces they hope to remain," corporate reputation "is an asset that companies cultivate, manage, and monetize." "It is not a quality integral to a company's emotional well-being, and its diminution exacts no psychological cost." Because corporations do not "feel burdens in the same way as living, breathing human beings," the bill of attainder analysis does not apply to them in the same way. The Commission thus rejects claims that the limitation on Commission equipment authorizations resembles a badge of infamy.

The functional test regarding punishment also persuades us that limitations on Commission-issued equipment authorizations as required by the Secure Equipment Act furthers nonpunitive legislative purposes, and thus is not punishment for bill of attainder purposes. The functional test asks "whether the statute, viewed in terms of the type and severity of burdens imposed, reasonably can be said to further nonpunitive legislative purposes." "It is not the severity of a statutory burden in absolute terms that demonstrates punitiveness so much as the magnitude of the burden relative to the purported nonpunitive purposes of the statute."

The Secure Equipment Act includes a prospective focus, prohibiting the future Commission authorization of those products and thereby preventing their use in U.S. communications networks because the covered communications equipment is understood, under triggers established by Congress, as "pos[ing] an unacceptable risk to the national security of the United States or the security and safety of United States persons." By restricting the Commission

from authorizing such equipment going forward, the Secure Equipment Act seeks to guard against future risks “to the national security of the United States or the security and safety of United States persons” that would arise if the equipment on the Covered List could be used by communications providers and customers, rather than punishing companies with equipment on the Covered List for past conduct. Thus, Congress ensured that the Commission could place equipment produced by any entity on the Covered List “if and only if,” among other things, it has capabilities associated with specific prospective national security risks—*i.e.*, of routing or redirecting traffic or permitting visibility into user data or packets, or causing remote disruption of the network—or “otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons.”

The burdens imposed by the Secure Equipment Act are also sufficiently tailored to the statute’s prophylactic purposes. The Supreme Court has warned that Congress must be given sufficient leeway in making policy decisions, lest the bill of attainder analysis “cripple the very process of legislating.” Congress is therefore not required to “precisely calibrate the burdens it imposes to . . . the threats it seeks to mitigate.” A statute does not fail the functional test unless it is “significantly overbroad,” such that it “pil[es] on . . . additional, entirely unnecessary burden[s],” or so underinclusive that it “seemingly burdens one among equals.” The standard is a high one because the inquiry remains whether the statute is so punitive that it “belies any purported nonpunitive goals.”

The Commission is unpersuaded by claims that the inability to obtain a Commission-issued equipment authorization for equipment on the Covered List should be considered “punishment” on the theories that the prohibitions are overbroad in scope or that there are narrower, less burdensome alternatives that could have been employed. This approach to bill of attainder review runs afoul of the Supreme Court’s warning against “cripp[ing] the very process of legislating.” The Bill of Attainder Clause does not command such a result. Precluding the Commission from granting authorizations for equipment on the Covered List has a clear nexus to the nonpunitive prophylactic purpose of guarding against risks “to the national security of the United States or the

security and safety of United States persons” that would arise if the equipment on the Covered List could be used by communications providers and customers.

Further, whether or not Congress or policymakers arguably have treated all the equipment on the Covered List in an identical manner in other contexts that have implicated security concerns does not demonstrate that treating them similarly in this context is punitive, as some allege. This is particularly true insofar as Congress might continue to learn from its experiences as it legislates against the backdrop of prior actions in this area. Under the applicable standard, “the question is not whether a burden is proportionate to the objective, but rather whether the burden is so disproportionate that it belies any purported nonpunitive goals.”

Nor is the Commission persuaded by Hikvision USA’s claim that Congress instead could have relied entirely on the framework used in the Federal Acquisition Supply Chain Security Act of 2018, under which “any company potentially subject to an exclusion or removal order would receive notice, including the relevant procedures and basis, a chance to respond, and an avenue for judicial review.” Determinations made under that framework are, in fact, one basis for inclusion in the Covered List, but the Commission is not persuaded that (or an analogous approach) needs to be the exclusive mechanism for identifying equipment presenting security risks that warrant triggering inclusion on the Covered List and the associated restriction on Commission equipment authorizations under the Secure Equipment Act. Given the wide latitude afforded Congress to choose between policy alternatives, it “does not matter that Congress arguably could have enacted different legislation in an effort to secure federal networks, because it cannot be legitimately suggested that the risks . . . were so feeble that no one could reasonably assert them except as a smoke screen for some invidious purpose.”

The Commission also rejects arguments that the Secure Equipment Act is underinclusive. To the extent that these arguments proceed from the assumption the Covered List only includes a limited, finite set of equipment from specific companies, they neglect the fact that the Covered List is designed by Congress to be updated over time—including reversing prior determinations—as additional determinations are made regarding security risk. This fact underscores that the statute’s purpose is to counter a

persistent threat, not to punish a particular company. Separately, the Supreme Court has explained that a law is not an unconstitutional attainder by virtue of its specificity, and there is no requirement that Congress pass only laws that are generally applicable. Such a requirement would leave Congress powerless to address national security threats directly whenever the person or entity posing the threat is specifically identifiable. The courts have therefore roundly—and rightly—rejected such an irrational result.

In addition, the Commission is unpersuaded by Hikvision USA’s claim that the Secure Equipment Act imposes punishment based on the Congressional motivations underlying its enactment. The Supreme Court has cautioned that “[j]udicial inquir[y] into Congressional motives [is] at best a hazardous matter” and that “the presumption of constitutionality” that attaches to a congressional enactment “forbids . . . [a] reading of the statute’s setting which will invalidate it over that which will save it.” Accordingly, “only the clearest proof” will render a statute unconstitutional based on congressional intent. “[I]solated statements” do not suffice. Yet commenters only muster isolated statements from individual legislators in support of their bill of attainder arguments here. The Commission finds such arguments particularly unpersuasive against the backdrop of the extensive history of concerns about U.S. safety and security in light of the sorts of equipment that are, and can be, included on the Covered List, which makes manifest its nonpunitive prophylactic purpose.

#### b. Equal Protection

The Commission rejects Hikvision USA’s arguments that our actions here violate constitutional requirements of equal protection. In particular, the Commission rejects the claim that the new equipment authorization rules target certain companies “on the basis of national origin or alienage” and should be subject to strict scrutiny under the equal protection clause. The premise underlying the inclusion of companies on the Covered List is that “communications equipment or service, . . . produced or provided by such entity poses an unacceptable risk to the national security of the United States or the security and safety of United States persons.” Although some commenters premise their equal protection concerns on the theory that they are being targeted merely because they are Chinese, the Commission observes that status as a Chinese company—or even a relationship with the Chinese

government—is not, standing alone, sufficient (or necessary) for inclusion on the Covered List. Ownership by, or connection with, the Chinese government is only one element of one possible basis for inclusion on the covered list, which also always critically depends on judgments about the technical characteristics and national security risks associated with the covered equipment and services. Because the treatment of these companies, as properly understood, does not turn on any suspect classifications, nor does it infringe fundamental constitutional rights, it only is subject to rational basis scrutiny under equal protection precedent. The treatment of these companies under the new equipment authorization rules adopted here readily satisfies rational basis review for the same reasons the Commission finds the new rules warranted more generally.

In the alternative, even assuming *arguendo* that strict scrutiny applied, the Commission concludes that standard would be satisfied here. Promoting national security is a compelling interest, as the Commission has recognized previously. The Commission also finds the new rules narrowly tailored to advance that interest. Those rules target the specific equipment identified as posing “an unacceptable risk to the national security of the United States or the security and safety of United States persons” under the framework of the Secure Networks Act, which involves either a judgment regarding national security risks made by Congress itself or through a specific executive branch analysis in that regard. Congress further concluded in the Secure Equipment Act that, in order to address those security risks, it was necessary for the Commission to deny equipment authorization for the equipment on the Covered List. The Commission’s analysis of the new rules more generally likewise affirms the need to take this step to guard against the national security risks associated with equipment on the Covered List. Given that, the Commission is unpersuaded by some commenters’ claims that the rules are overinclusive. The Commission also does not find the rules underinclusive. Contrary to some commenters’ claims, the Covered List and the Commission’s associated equipment authorization rules do not narrowly focus on companies linked to the Chinese government to the exclusion of companies from other countries, which arguably present similar security risks. While those comments myopically focus

on the equipment actually included on the Covered List at a given moment in time, the Covered List is an evolving inventory of certain communications equipment and services found to present an unreasonable security risk under the Secure Networks Act’s framework. The Commission expects that evidence of national security risks associated with other communications equipment and services similar to that posed by the equipment and services already on the Covered List likewise would lead to determinations under the review frameworks that would trigger inclusion of those equipment and services on the Covered List, and the Commission sees no basis in the record to suppose otherwise.

#### c. Takings

Nor is the Commission persuaded by Hikvision USA that the rules the Commission adopted in this proceeding represent a taking of property in violation of the Fifth Amendment. For one, the Commission finds that the rules do not represent a *per se* taking. The Commission’s rules do not appropriate the equipment at issue for government use, nor is the Commission persuaded that the rules deny owners of the relevant equipment “all economically beneficial use[s]” of their property, given that the lack of Commission equipment authorization does not preclude it from, among other things, marketing, selling, or using the equipment outside the U.S.

The Commission also rejects assertions that its rules represent a regulatory taking. The principal factors a court will review in determining whether a governmental regulation effects a taking are: (a) the character of the governmental action; (b) the economic impact of that action; and (c) the action’s interference, if any, with investment-backed expectations. Regarding the first factor, as noted above the rules adopted here do not appropriate the relevant equipment for government use, but instead promote a significant common good by promoting national security and protecting the nation’s communications infrastructure from potential security threats. With respect to the second factor, even assuming *arguendo* some diminution in value of the equipment actually addressed by the Commission’s actions in the Report and Order—*i.e.*, equipment that has not yet received Commission authorization, that is merely necessary—but not sufficient—to demonstrate a regulatory taking. Nor is the Commission persuaded that its rules interfere with reasonable investment-backed expectations under the third factor. The equipment at issue has long

been subject to Commission authorization requirements, and the Supreme Court has recognized that for property that “had long been subject to federal regulation” there was no “reasonable basis to expect” that the regulatory regime would not change. Indeed, the reasonableness of any expectations regarding the not-yet-authorized equipment addressed by the Report and Order is especially doubtful, given the years of legislative and regulatory focus on possible security-related restrictions on such equipment. Particularly in light of “the heavy burden placed upon one alleging a regulatory taking,” the Commission finds no basis to find a regulatory taking on the record here.

#### d. Separation of Powers

The Commission also is unpersuaded by Hikvision that Commission actions would be invalid on separation of powers grounds. In particular, Hikvision contends that “[b]ecause the FCC Commissioners are appointed by the President and wield significant powers that are executive in nature, but are not removable at will by the President, their status may well conflict with the Constitution’s separation of powers” in the event that certain recent Supreme Court precedent regarding Presidential removal were “to be applied to multi-member agencies like the FCC.” But insofar as the Supreme Court has not gone that far—as Hikvision itself observes—the Commission is not persuaded to find constitutional concerns in that regard ourselves.

#### 3. WTO and Mutual Recognition Agreements

*World Trade Organization (WTO)*. In its comments, the People’s Republic of China (PRC) argues that placing only Chinese companies on the Covered List violates non-discriminatory principles in the World Trade Organization/Technical Barriers to Trade (WTO/TBT) agreement. In particular, it asserts article 2.1 of that agreement requires that member countries ensure that, in their technical regulations, products imported from other members must be accorded no less favorable treatment, and that prohibiting the authorization of equipment and services on the Covered List violates WTO/TBT transparency principles in the absence of a public technical standard and measurement index. Similar concerns are raised by Dahua, which urges the Commission to consider whether its proposed rule may implicate U.S. obligations through the WTO or the General Agreement on Tariffs and Trade.



The Commission finds that, contrary to those assertions, the Commission's actions in this proceeding are consistent with the United States' international obligations under the WTO/TBT agreement. As discussed above and clearly laid out in statute, the Commission is required to include on the Covered List equipment and services based solely on determinations by four enumerated U.S. Government sources relating to national security. Under the relevant statutes, those determinations are not made, as suggested by these commenters, on the basis of nationality but are made based on fact-specific reviews whether the relevant equipment and services are found to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons, and not on sweeping determinations on the basis of nationality. Indeed, the March 2022 update to the Covered List includes equipment and services from countries other than China. Finally, the Commission notes that nearly all products from China will remain eligible for equipment authorization under the Commission's new rules. Therefore, the Commission finds that the commenters' concerns are without merit.

*Potential Impact on Global Trade and Mutual Recognition Agreements.* Noting the "robust" international trade in consumer electronics, CTA asks that the Commission consider how changes to its equipment authorization program would impact relationships and policies with global trade partners, including possible retaliatory actions by China. In particular, CTA asks that the Commission consider potential impacts on the mutual recognition agreements (MRAs) that expedite trade, including the recognitions that participating countries give to each other's testing labs and certification bodies in order to speed time to market and decrease regulatory costs to manufacturers. Dahua also requests that the Commission consider whether adoption of its proposed rules could cause China to take retaliatory trade action.

The Commission has considered whether the proposed rules would have impacts on the relationships with the Commission's global trade partners, and in particular on MRAs. MRAs are expressly designed with recognition that equipment authorization processes are continually evolving. MRAs establish a process for the recognition of conformity assessment bodies and the acceptance of conformity assessment results without fixing the precise requirements to which products must

conform, as these requirements evolve over time. They also typically include clauses on the preservation of regulatory authority in recognition of the need for future updates to such requirements. The changes to the Commission's rules adopted in the Report and Order merely update the requirements for authorizing equipment, without affecting which conformity assessment bodies may do so. Therefore, the Commission finds that the changes made here are consistent with the existing MRAs.

More generally, the Commission finds that the possibility of retaliatory trade action is speculative, and that the expected benefits of adopting the Commission's new rules outweigh any such concerns. As mentioned above, nearly all products from China that were previously eligible for equipment authorization will remain so under the Commission's new rules, and so the impact on international trade of adopting these new rules is likely to be small.

#### 4. Claims That Commission Action Is Arbitrary and Capricious

The Commission rejects the arguments of Hikvision USA and Dahua USA that the Commission's actions in this proceeding are arbitrary and capricious. Hikvision USA argues that the Commission's regulations prohibition authorization of "covered" equipment is arbitrary and capricious because the regulations address highly speculative, unsubstantiated security risks about Hikvision equipment such as its video surveillance equipment, which Hikvision USA contends is secure as deployed. Hikvision USA also contends that the regulations are arbitrary and capricious because of the highly disruptive effects on American businesses. Among other things, Dahua USA contends that the proposed rules fall outside of the Commission's statutory authority and that the Commission should not, in any event, prohibit all of Dahua's equipment from authorization given that section 889(f)(3)(B) of the 2019 NDAA only concerns Dahua equipment to the extent used for specific purposes. Considering the Commission's discussion of the record before us, and the Commission's reasoned analyses explaining the elements of the decisions that the Commission adopted in this proceeding with regard to Hikvision and Dahua equipment, the Commission need not further address the claims that Hikvision USA and Dahua USA raise in general terms here.

#### E. Outreach

In the *NPRM*, the Commission sought comment on what types of actions or activities (e.g., outreach and education) the Commission should take to inform all parties potentially affected by the Commission's changes to the equipment certification and SDoC rules, as well as any other rule revisions, to help ensure that they understand the changes and will comply with the prohibitions that the Commission adopted with respect to the authorization of "covered" equipment.

As discussed above, the Commission will provide clear guidance on the Commission's website regarding what constitutes "covered" equipment for purposes of the equipment authorization program and the prohibition on authorization that the Commission adopted in the Report and Order. The Commission also noted that OET and PSHSB will issue a Public Notice on such guidance, and that any updates will also be issued pursuant to a Public Notice.

With regard to the revisions affecting the SDoC process in particular, the Commission endeavors to assist each responsible party in identifying equipment that can no longer be authorized through the SDoC procedures, while also ensuring that each responsible party is accountable for any misrepresentations or violation of the prohibition that the Commission is implementing. Because SDoC procedure does not routinely involve direct interaction with the Commission, and because the rules specify who may act as a "responsible party," in the *NPRM*, the Commission asked several questions related to disseminating the new SDoC limitations and requirements to the responsible parties. Commenters were largely silent on those questions and, as previously discussed, the Commission does not routinely maintain information for SDoC equipment thus making direct outreach difficult. The Commission finds that because most or all entities engaged in the SDoC process are familiar with FCC procedures and their obligations to comply with the Commission's requirements, it is sufficient to provide initial notification via publication of the Report and Order on the FCC website along with publication in the **Federal Register** of a summary of this change in procedure. Following implementation of the newly adopted procedures, the Commission encourages industry and other interested parties to reach out to the Commission with any questions or concerns regarding these procedures. The Commission directs OET to monitor

such inquiries and to issue additional guidance as needed.

## II. Interim Freeze Order

Because of the revisions the Commission adopted in the Report and Order to the part 2 equipment authorization rules and procedures to prohibit authorization of any “covered” equipment specified in the Covered List, the Commission also adopted an interim freeze on further processing or grant of equipment authorization applications for equipment that is produced by any entity identified on the Covered List as producing “covered” equipment. This freeze was effective on release of the Report and Order, lasting only until the Commission provides notice that the rules adopted in the Report and Order have become effective. The Commission concluded that this action was necessary and in the public interest in order to avoid submission of new applications seeking authorization of equipment following the adoption of the Report and Order but before the rules would otherwise go into effect. The Commission took this action because “covered” equipment has been determined to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons, and the freeze accordingly serves the public interest.

Effective as of the adoption of the Report and Order, and because the Commission’s rules, which are designed to determine which if any applications from the entities whose equipment is currently on the Covered List do not involve “covered” equipment, were not yet in effect, TCBs were directed to cease issuing equipment certifications to any of the entities identified on the Covered List—i.e., the five named entities—Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company—and their subsidiaries or affiliates. OET was directed to issue pre-approval guidance relating to the prohibition against certification of this equipment to the TCBs. The Commission reminded TCBs that they were designated by the Commission “to certify equipment in accordance with Commission rules and policies,” and are required to “conform their testing and certification processes and procedures to comply with any changes the Commission made in its rules and requirements.” The Commission expected that TCBs, applicants, and responsible parties would be vigilant in taking appropriate actions to implement this freeze.

The purpose of this interim freeze was to preserve the current landscape of authorized equipment pending the effective date of the Commission’s revisions to the equipment authorization process, which would serve to protect the public interest, including the national security and public safety of United States persons. This interim procedure is consistent with the Commission’s practice of taking steps to ensure that parties do not take advantage of the period between the adoption of new rules and the date those rules become effective. The freeze was limited to the brief time period during which the rules implementing the statutory mandate were not yet effective. Finally, if the Covered List is updated to revise the entities identified on the Covered List as producing “covered” equipment, this procedural freeze would be revised accordingly. The Commission delegated authority to OET to modify or extend the freeze as appropriate.

## III. Ordering Clauses

Accordingly, *it is ordered*, pursuant to the authority found in sections 4(i), 301, 302, 303, 309(j), 312, 403, and 503 of the Communications Act of 1934, as amended, 47 U.S.C. 154(i), 301, 302a, 303, 309(j), 312, 403, 503, and the Secure Equipment Act of 2021, Public Law 117–55, 135 Stat. 423, that the Report and Order, Order, and Further Notice of Proposed Rulemaking *is hereby adopted*.

*It is further ordered* that the amendments of parts 2 and 15 of the Commission’s rules as set forth in Appendix A *are adopted*, effective on the date of publication in the **Federal Register**.

*It is further ordered* that authority is delegated to the Office of Engineering and Technology and the Public Safety and Homeland Security Bureau to develop and inform applicants for equipment authorization, TCBs, and other interested parties with more specific and detailed information on the categories, types, and characteristics of equipment that constitutes “telecommunications equipment” for purposes of the prohibition on future authorization of “covered” equipment identified on the Covered List, and to make such information available on the Commission’s website, and to revise that information as appropriate.

*It is further ordered* that authority is delegated to the Office of Engineering and Technology and the Public Safety and Homeland Security Bureau to adopt appropriate procedures for streamlined revocation proceedings and to revoke

authorizations consistent with the provisions of the Report and Order.

*It is further ordered* that the interim freeze shall be effective on release, and authority is delegated to the Office of Engineering and Technology to extend or modify the interim freeze, as appropriate.

*It is further ordered* that the Commission’s Consumer and Governmental Affairs Bureau, Reference Information Center, *shall send* a copy of the Report and Order, Order, and Further Notice of Proposed Rulemaking, including the Initial and Final Regulatory Flexibility Analysis, to Congress and the Government Accountability Office pursuant to the Congressional Review Act, *see* 5 U.S.C. 801(a)(1)(A).

## List of Subjects

### 47 CFR Part 2

Communications equipment, Radio, Telecommunications.

### 47 CFR Part 15

Communications equipment

Federal Communications Commission.

**Katura Jackson,**

*Federal Register Liaison Officer, Office of the Secretary.*

## Final Rules

For the reasons discussed in the preamble, the Federal Communications Commission amends 47 CFR parts 2 and 15 as follows:

## PART 2—FREQUENCY ALLOCATIONS AND RADIO TREATY MATTERS; GENERAL RULES AND REGULATIONS

■ 1. The authority citation for part 2 continues to read as follows:

**Authority:** 47 U.S.C. 154, 302a, 303, and 336 unless otherwise noted.

■ 2. Amend § 2.901 by revising paragraph (a) to read as follows:

### § 2.901 Basis and purpose.

(a) In order to carry out its responsibilities under the Communications Act and the various treaties and international regulations, and in order to promote efficient use of the radio spectrum, the Commission has developed technical standards and other requirements for radio frequency equipment and parts or components thereof. The technical standards applicable to individual types of equipment are found in that part of the rules governing the service wherein the equipment is to be operated. In addition to the technical standards provided, the rules governing the service may require that such equipment be authorized

under Supplier's Declaration of Conformity or receive a grant of certification from a Telecommunication Certification Body.

■ 3. Add § 2.903 to subpart J to read as follows:

**§ 2.903 Prohibition on authorization of equipment on the Covered List.**

(a) All equipment on the Covered List, as established pursuant to § 1.50002 of this chapter, is prohibited from obtaining an equipment authorization under this subpart. This includes:

(1) Equipment that would otherwise be subject to certification procedures;

(2) Equipment that would otherwise be subject to Supplier's Declaration of Conformity procedures; and

(3) Equipment that would otherwise be exempt from equipment authorization.

(b) Each entity named on the Covered List as producing covered communications equipment, as established pursuant to § 1.50002 of this chapter, must provide to the Commission the following information: the full name, mailing address or physical address (if different from mailing address), email address, and telephone number of each of that named entity's associated entities (*e.g.*, subsidiaries or affiliates) identified on the Covered List as producing covered communications equipment.

(1) Each entity named on the Covered List as producing covered communications equipment must provide the information described in paragraph (b) of this section no later than March 8, 2023;

(2) Each entity named on the Covered List as producing covered communications equipment must provide the information described in paragraph (b) of this section no later than 30 days after the effective date of each updated Covered List; and

(3) Each entity named on the Covered List as producing covered communications equipment must notify the Commission of any changes to the information described in paragraph (b) of this section no later than 30 days after such change occurs.

(c) For purposes of implementing this subpart with regard to the prohibition on authorization of communications equipment on the Covered List, the following definitions apply:

*Affiliate.* The term "affiliate" means an entity that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another entity; for purposes of this paragraph, the term 'own' means to have, possess, or otherwise control an equity interest (or

the equivalent thereof) of more than 10 percent.

*Subsidiary.* The term "subsidiary" means any entity in which another entity directly or indirectly:

(i) Holds de facto control; or

(ii) Owns or controls more than 50 percent of the outstanding voting stock.

(d) The Commission delegates authority to the Office of Engineering and Technology and the Public Safety and Homeland Security Bureau to develop and provide additional clarifications as appropriate regarding implementation of the prohibition on authorization of covered communications equipment. The Office of Engineering and Technology and Public Safety and Homeland Security Bureau will issue through Public Notice, and publish on the Commission's website, the Commission's relevant guidance on covered communications equipment, as well as further clarifications, and will update and maintain this information as appropriate.

■ 4. Amend § 2.906 by revising paragraph (a) and adding paragraph (d) to read as follows:

**§ 2.906 Supplier's Declaration of Conformity.**

(a) Supplier's Declaration of Conformity (SDoC) is a procedure where the responsible party, as defined in § 2.909, makes measurements or completes other procedures found acceptable to the Commission to ensure that the equipment complies with the appropriate technical standards and other applicable requirements. Submittal to the Commission of a sample unit or representative data demonstrating compliance is not required unless specifically requested pursuant to § 2.945.

(d) Notwithstanding other parts of this section, equipment otherwise subject to the Supplier's Declaration of Conformity process that is produced by any entity identified on the Covered List, established pursuant to § 1.50002 of this chapter, as producing covered communications equipment is prohibited from obtaining equipment authorization through that process. The rules governing certification apply to authorization of such equipment.

■ 5. Amend § 2.907 by adding paragraph (c) to read as follows:

**§ 2.907 Certification.**

(c) Any equipment otherwise eligible for authorization pursuant to the Supplier's Declaration of Conformity, or exempt from equipment authorization,

produced by any entity identified on the Covered List, established pursuant to § 1.50002 of this chapter, as producing covered communications equipment must obtain equipment authorization through the certification process.

■ 6. Amend § 2.909 by revising paragraph (a) to read as follows:

**§ 2.909 Responsible Party.**

(a) In the case of equipment that requires the issuance of a grant of certification, the party to whom that grant of certification is issued is responsible for the compliance of the equipment with the applicable technical and other requirements. If any party other than the grantee modifies the radio frequency equipment and that party is not working under the authorization of the grantee pursuant to § 2.929(b), the party performing the modification is responsible for compliance of the product with the applicable administrative and technical provisions in this chapter.

\* \* \* \* \*

■ 7. Amend § 2.911 by revising paragraph (b) and by adding paragraphs (d)(5) through (7) to read as follows:

**§ 2.911 Application requirements.**

\* \* \* \* \*

(b) A TCB shall submit an electronic copy of each equipment authorization application to the Commission pursuant to § 2.962(f)(8) on a form prescribed by the Commission at <https://www.fcc.gov/eas>.

\* \* \* \* \*

(d) \* \* \*

(5) The applicant shall provide a written and signed certification that, as of the date of the filing of the application with a TCB:

(i) The equipment for which the applicant seeks equipment authorization through certification is not prohibited from receiving an equipment authorization pursuant to § 2.903; and

(ii) An affirmative or negative statement as to whether the applicant is identified on the Covered List, established pursuant to § 1.50002 of this chapter, as an entity producing covered communications equipment.

(6) If the Covered List established pursuant to § 1.50002 of this chapter is modified after the date of the written and signed certification required by paragraph (d)(5) of this section but prior to grant of the authorization, then the applicant shall provide a new written and signed certification as required by paragraph (d)(5) of this section.

(7) The applicant shall designate an agent located in the United States for

the purpose of accepting service of process on behalf of the applicant.

(i) The applicant shall provide a written certification:

(A) Signed by both the applicant and its designated agent for service of process, if different from the applicant;

(B) Acknowledging the applicant's consent and the designated agent's obligation to accept service of process in the United States for matters related to the applicable equipment, and at the physical U.S. address and email address of its designated agent; and

(C) Acknowledging the applicant's acceptance of its obligation to maintain an agent for service of process in the United States for no less than one year after either the grantee has permanently terminated all marketing and importation of the applicable equipment within the U.S., or the conclusion of any Commission-related administrative or judicial proceeding involving the equipment, whichever is later.

(ii) An applicant located in the United States may designate itself as the agent for service of process.

\* \* \* \* \*

■ 8. Amend § 2.915 by revising paragraph (a)(1) to read as follows:

**§ 2.915 Grant of application.**

(a) \* \* \*

(1) The equipment is capable of complying with pertinent technical standards of the rule part(s) under which it is to be operated as well as other applicable requirements; and

\* \* \* \* \*

■ 9. Amend § 2.929 by adding paragraph (b)(3) and revising paragraph (c) to read as follows:

**§ 2.929 Changes in name, address, ownership or control of grantee.**

\* \* \* \* \*

(b) \* \* \*

(3) Such second party must not be an entity identified on the Covered List established pursuant to § 1.50002 of this chapter.

(c) Whenever there is a change in the name and/or address of the grantee of certification, or a change in the name, mailing address or physical address (if different from mailing address), email address, or telephone number of the designated agent for service of process in the United States, notice of such change(s) shall be submitted to the Commission via the internet at <https://www.fcc.gov/eas> within 30 days after the beginning use of the new name, mailing address or physical address (if different from mailing address), email address, or telephone number and include:

(1) A written and signed certification that, as of the date of the filing of the notice, the equipment to which the change applies is not prohibited from receiving an equipment authorization pursuant to § 2.903;

(2) An affirmative or negative statement as to whether the applicant is identified on the Covered List, established pursuant to § 1.50002 of this chapter, as an entity producing covered communications equipment; and

(3) The written and signed certifications required under § 2.911(d)(7).

\* \* \* \* \*

■ 10. Amend § 2.932 by adding paragraph (e) to read as follows:

**§ 2.932 Modification of equipment.**

\* \* \* \* \*

(e) All requests for permissive changes shall be accompanied by:

(1) A written and signed certification that, as of the date of the filing of the request for permissive change, the equipment to which the change applies is not prohibited from receiving an equipment authorization pursuant to § 2.903;

(2) An affirmative or negative statement as to whether the applicant is identified on the Covered List, established pursuant to § 1.50002 of this chapter, as an entity producing covered communications equipment; and

(3) The written and signed certifications required under § 2.911(d)(7).

■ 11. Amend § 2.938 by revising paragraph (b) introductory text, redesignating paragraphs (b)(1) through (11) as paragraphs (b)(1)(i) through (xi), and adding paragraphs (b)(1) introductory text and (b)(2) to read as follows:

**§ 2.938 Retention of records.**

\* \* \* \* \*

(b) For equipment subject to Supplier's Declaration of Conformity, the responsible party shall, in addition to the requirements in paragraph (a) of this section, maintain the following records:

(1) Measurements made on an appropriate test site that demonstrates compliance with the applicable regulations in this chapter. The record shall:

\* \* \* \* \*

(2) A written and signed certification that, as of the date of first importation or marketing of the equipment, the equipment for which the responsible party maintains Supplier's Declaration of Conformity is not produced by any entity identified on the Covered List,

established pursuant to § 1.50002 of this chapter, as producing covered communications equipment.

\* \* \* \* \*

■ 12. Amend § 2.939 by revising paragraph (b) and adding paragraph (d) to read as follows:

**§ 2.939 Revocation or withdrawal of equipment authorization.**

\* \* \* \* \*

(b) Revocation of an equipment authorization shall be made in the same manner as revocation of radio station licenses, except as provided in paragraph (d) of this section.

\* \* \* \* \*

(d) Notwithstanding other provisions of § 2.939, to the extent a false statement or representation is made in the equipment certification application (see §§ 2.911(d)(5)–(7), 2.932, 2.1033, and 2.1043), or in materials or responses submitted in connection therewith, that the equipment in the subject application is not prohibited from receiving an equipment authorization pursuant to § 2.903, and the equipment certification or modification was granted, if the Commission subsequently determines that the equipment is covered communications equipment, the Commission will revoke such authorization.

(1) If the Office of Engineering and Technology and the Public Safety and Homeland Security Bureau determine that particular authorized equipment is covered communications equipment, and that the certification application for that equipment contained a false statement or representation that the equipment was not covered communications equipment, they will provide written notice to the grantee that a revocation proceeding is being initiated and the grounds under consideration for such revocation.

(2) The grantee will have 10 days in which to respond in writing to the reasons cited for initiating the revocation proceeding. The Office of Engineering and Technology and the Public Safety and Homeland Security Bureau will then review the submissions, request additional information as may be appropriate, and make their determination as to whether to revoke the authorization, providing the reasons for such decision.

■ 13. Amend § 2.1033 by:

■ a. Revising paragraph (b)(1);

■ b. Redesignating paragraphs (b)(2) through (14) as paragraphs (b)(5) through (17), and adding new paragraphs (b)(2) through (4);

■ c. Revising paragraph (c)(1);

■ d. Redesignating paragraphs (c)(2) through (21) as paragraphs (c)(5)

through (24), and adding new paragraphs (c)(2) through (4).

The revisions and additions read as follows:

**§ 2.1033 Application for Certification.**

\* \* \* \* \*

(b) \* \* \*

(1) The full name, mailing address and physical address (if different from mailing address), email address, and telephone number of:

(i) The applicant for certification; and

(ii) The applicant's agent for service of process in the United States for matters relating to the authorized equipment.

(2) A written and signed certification that, as of, the filing date of the notice, the equipment to which the change applies is not prohibited from receiving an equipment authorization pursuant to § 2.903;

(3) An affirmative or negative statement as to whether the applicant is identified on the Covered List, established pursuant to § 1.50002 of this chapter, as an entity producing covered communications equipment; and

(4) The written and signed certifications required by § 2.911(d)(7).

\* \* \* \* \*

(c) \* \* \*

(1) The full name, mailing address and physical address (if different from mailing address), email address, and telephone number of:

(i) The applicant for certification; and

(ii) The applicant's agent for service of process in the United States for matters relating to the authorized equipment.

(2) A written and signed certification that, as of the filing date of the notice, the equipment to which the change applies is not prohibited from receiving an equipment authorization pursuant to § 2.903.

(3) An affirmative or negative statement as to whether the applicant is identified on the Covered List, established pursuant to § 1.50002 of this chapter, as an entity producing covered communications equipment.

(4) The written and signed certifications required by § 2.911(d)(7).

\* \* \* \* \*

■ 14. Amend § 2.1043 by revising paragraphs (b)(2) and (3) to read as follows:

**§ 2.1043 Changes in certificated equipment.**

\* \* \* \* \*

(b) \* \* \*

(2) A Class II permissive change includes those modifications which degrade the performance characteristics as reported to the Commission at the time of the initial certification. Such degraded performance must still meet

the minimum requirements of the applicable rules.

(i) When a Class II permissive change is made by the grantee, the grantee shall provide:

(A) Complete information and the results of tests of the characteristics affected by such change;

(B) A written and signed certification expressly stating that, as of the filing date, the equipment subject to the permissive change is not prohibited from receiving an equipment authorization pursuant to § 2.903;

(C) An affirmative or negative statement as to whether the applicant is identified on the Covered List, established pursuant to § 1.50002 of this chapter, as an entity producing covered communications equipment;

(D) The full name, mailing address and physical address (if different from mailing address), email address, and telephone number of the grantee's designated agent for service of process in the United States for matters relating to the authorized equipment; and

(E) The written and signed certifications required by § 2.911(d)(7).  
(ii) The modified equipment shall not be marketed under the existing grant of certification prior to acknowledgement that the change is acceptable.

(3) A Class III permissive change includes modifications to the software of a software defined radio transmitter that change the frequency range, modulation type or maximum output power (either radiated or conducted) outside the parameters previously approved, or that change the circumstances under which the transmitter operates in accordance with Commission rules.

(i) When a Class III permissive change is made, the grantee shall provide:

(A) A description of the changes and test results showing that the equipment complies with the applicable rules with the new software loaded, including compliance with the applicable RF exposure requirements.

(B) A written and signed certification expressly stating that, as of the date of the filing, the equipment subject to the permissive change is not prohibited from receiving an equipment authorization pursuant to § 2.903;

(C) An affirmative or negative statement as to whether the applicant is identified on the Covered List, established pursuant to § 1.50002 of this chapter, as an entity producing covered communications equipment;

(D) The full name, mailing address and physical address (if different from mailing address), email address, and telephone number of the grantee's designated agent for service of process

in the United States for matters relating to the authorized equipment; and

(E) The written and signed certifications required by § 2.911(d)(7).

(ii) The modified software shall not be loaded into the equipment, and the equipment shall not be marketed with the modified software under the existing grant of certification, prior to acknowledgement that the change is acceptable.

(iii) Class III changes are permitted only for equipment in which no Class II changes have been made from the originally approved device.

\* \* \* \* \*

■ 15. Amend § 2.1072 by revising paragraph (a) to read as follows:

**§ 2.1072 Limitation on Supplier's Declaration of Conformity.**

(a) Supplier's Declaration of Conformity signifies that the responsible party, as defined in § 2.909, has determined that the equipment has been shown to comply with the applicable technical standards and other applicable requirements if no unauthorized change is made in the equipment and if the equipment is properly maintained and operated. Compliance with these standards and other applicable requirements shall not be construed to be a finding by the responsible party with respect to matters not encompassed by the Commission's rules.

\* \* \* \* \*

**PART 15—RADIOFREQUENCY DEVICES**

■ 18. The authority citation for part 15 continues to read as follows:

**Authority:** 47 U.S.C. 154, 302a, 303, 304, 307, 336, 544a, and 549.

■ 19. Amend § 15.103 by revising the introductory text and adding paragraph (j) to read as follows:

**§ 15.103 Exempted devices.**

Except as provided in paragraph (j) of this section, the following devices are subject only to the general conditions of operation in §§ 15.5 and 15.29, and are exempt from the specific technical standards and other requirements contained in this part. The operator of the exempted device shall be required to stop operating the device upon a finding by the Commission or its representative that the device is causing harmful interference. Operation shall not resume until the condition causing the harmful interference has been corrected. Although not mandatory, it is strongly recommended that the manufacturer of an exempted device endeavor to have

the device meet the specific technical standards in this part.

\* \* \* \* \*

(j) Notwithstanding other provisions of this section, the rules governing certification apply to any equipment produced by any entity identified on the Covered List, as established pursuant to § 1.50002 of this chapter, as producing covered communications equipment.

\* \* \* \* \*

[FR Doc. 2022-28263 Filed 2-3-23; 8:45 am]

BILLING CODE 6712-01-P

## DEPARTMENT OF COMMERCE

### National Oceanic and Atmospheric Administration

#### 50 CFR Part 622

[Docket No. 140819687-5583-02; RTID 0648-XC734]

#### Coastal Migratory Pelagic Resources of the Gulf of Mexico and Atlantic Region; 2022-2023 Commercial Trip Limit Reduction for Spanish Mackerel in the Atlantic Southern Zone

**AGENCY:** National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

**ACTION:** Temporary rule; trip limit reduction.

**SUMMARY:** NMFS reduces the commercial trip limit for the Atlantic migratory group of Spanish mackerel in the southern zone of the Atlantic exclusive economic zone (EEZ) to 1,500 lb (680 kg) in round or gutted weight per day. This commercial trip limit reduction is necessary to increase the socioeconomic benefits of the fishery.

**DATES:** This temporary rule is effective from 6 a.m. eastern time on February 4, 2023, until 12:01 a.m. eastern time on March 1, 2023.

**FOR FURTHER INFORMATION CONTACT:** Mary Vara, NMFS Southeast Regional Office, telephone: 727-824-5305, or email: [mary.vara@noaa.gov](mailto:mary.vara@noaa.gov).

**SUPPLEMENTARY INFORMATION:** The fishery for coastal migratory pelagic fish in the Atlantic EEZ includes king mackerel, Spanish mackerel, and cobia on the east coast of Florida, and is managed under the Fishery Management Plan for the Coastal Migratory Pelagic Resources of the Gulf of Mexico and Atlantic Region (FMP). The FMP was prepared by the Gulf of Mexico and South Atlantic Fishery Management Councils and is implemented by NMFS under the authority of the Magnuson-Stevens

Fishery Conservation and Management Act (Magnuson-Stevens Act) by regulations at 50 CFR part 622. All weights described for the Atlantic migratory group of Spanish mackerel (Atlantic Spanish mackerel) apply as either round or gutted weight.

For management purposes, the commercial sector of Atlantic Spanish mackerel is divided into northern and southern zones. The southern zone consists of Federal waters off South Carolina, Georgia, and the east coast of Florida, as specified in 50 CFR 622.369(b)(2)(ii). The southern zone boundaries for Atlantic Spanish mackerel extend from the border of North Carolina and South Carolina, which is a line extending in a direction of 135°34'55" from true north beginning at 33°51'07.9" N latitude and 78°32'32.6" W longitude to the intersection point with the outward boundary of the EEZ, to the border of Miami-Dade and Monroe Counties in Florida at 25°20'24" N latitude.

The southern zone commercial quota for Atlantic Spanish mackerel is 2,667,330 lb (1,209,881 kg). Seasonally variable trip limits are based on an adjusted commercial quota of 2,417,330 lb (1,096,482 kg). The adjusted commercial quota is calculated to allow continued harvest in the southern zone at a set rate for the remainder of the current fishing year, through February 28, 2023, in accordance with 50 CFR 622.385(b)(2).

As specified at 50 CFR 622.385(b)(1)(ii)(B), after 75 percent of the adjusted commercial quota of Atlantic Spanish mackerel for the southern zone is reached or is projected to be reached, Atlantic Spanish mackerel in or from the EEZ in the southern zone may not be possessed on board or landed from a vessel that has been issued a Federal permit for Atlantic Spanish mackerel in amounts exceeding 1,500 lb (680 kg) per day.

NMFS has determined that 75 percent of the adjusted commercial quota for Atlantic Spanish mackerel for the southern zone will be reached by February 4, 2023. Accordingly, the commercial trip limit of 1,500 lb (680 kg) per day applies to Atlantic Spanish mackerel harvested in or from the EEZ in the southern zone effective from 6 a.m. eastern time on February 4, 2023, until 12:01 a.m. eastern time on March 1, 2023, unless NMFS announces a subsequent change through a notification in the **Federal Register**.

#### Classification

NMFS issues this action pursuant to section 305(d) of the Magnuson-Stevens Act. This action is required by 50 CFR

622.385(b)(1)(ii)(B), which was issued pursuant to section 304(b) of the Magnuson-Stevens Act, and is exempt from review under Executive Order 12866.

Pursuant to 5 U.S.C. 553(b)(B), there is good cause to waive prior notice and an opportunity for public comment on this action, as notice and comment is unnecessary and contrary to the public interest. Such procedures are unnecessary because the regulations associated with the commercial trip limit for Atlantic Spanish mackerel have already been subject to notice and public comment, and all that remains is to notify the public of the commercial trip limit reduction. Prior notice and opportunity for public comment on this action is contrary to the public interest because of the time required to provide notice and an opportunity for public comment. There is a need to immediately implement the commercial trip limit reduction to increase the socioeconomic benefits of the fishery. The capacity of the fishing fleet allows for rapid harvest of the commercial quota, and any delay in reducing the commercial trip limit could result in the commercial quota being reached. If the commercial quota is reached, NMFS is required to implement further fishery restrictions, thereby limiting the socioeconomic benefits of the fishery.

For the reasons stated earlier, there is good cause under 5 U.S.C. 553(d)(3) to waive the 30-day delay in effectiveness of this action.

**Authority:** 16 U.S.C. 1801 *et seq.*

Dated: February 1, 2023.

**Ngagne Jafnar Gueye,**  
*Acting Director, Office of Sustainable Fisheries, National Marine Fisheries Service.*

[FR Doc. 2023-02439 Filed 2-1-23; 4:15 pm]

BILLING CODE 3510-22-P

## DEPARTMENT OF COMMERCE

### National Oceanic and Atmospheric Administration

#### 50 CFR Part 648

[Docket No. 230119-0020]

RIN 0648-BJ04

#### Magnuson-Stevens Act Provisions; Fisheries of the Northeastern United States; Omega Electronic Mesh Measurement Gauge Method for Measuring Net Mesh Size

**AGENCY:** National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.