

# FCC to Vote on International Section 214 Overhaul: What Authorization Holders Need to Know

October 26, 2026

The Federal Communications Commission (FCC) will vote on October 29, 2026, on a draft Report and Order and Further Notice of Proposed Rulemaking in the Evolving Risks proceeding (IB Docket No. 23-119). The draft, circulated October 8, is not final FCC action and may change.<sup>1</sup>

## Status, Sunshine period and effective dates

The item is not final FCC action and remains subject to change. The proceeding is permit-but-disclose. The FCC is expected to release the Sunshine Agenda for the October 29 meeting on October 22, 2026; under the FCC’s rules, presentations to decision-makers on the item are prohibited beginning the day after that release – October 23, 2026 – and remain prohibited until the FCC releases the text of the adopted item.<sup>2</sup>

If adopted, the rules would take effect 60 days after Federal Register publication, except that the amendments to sections 63.18, 63.19, 63.21 and 63.24 – which contain nearly all of the new obligations – and the one-time collection take effect only after the Office of Management and Budget (OMB) completes Paperwork Reduction Act review. The Office of International Affairs (OIA) will announce those dates and the collection deadline. Pending applications need not be amended, but grants will be conditioned on the new rules, and applicants must certify acceptance of the routine conditions within 30 days of the effective date. Unless noted, this alert describes what the FCC “would” adopt; Further Notice items remain proposals only.

## Key deadlines

| Obligation                                                                      | Who                                  | Deadline (from effective date unless noted)                                   |
|---------------------------------------------------------------------------------|--------------------------------------|-------------------------------------------------------------------------------|
| Certify acceptance of amended conditions; cyber and Covered List certifications | Applicants pending on effective date | 30 days                                                                       |
| Certify future cybersecurity compliance                                         | Existing holders                     | 30 days                                                                       |
| Submit one-time information collection                                          | Existing holders                     | No fewer than 30 days after the collection’s effective date (OIA to announce) |

|                                                   |                          |                                                                  |
|---------------------------------------------------|--------------------------|------------------------------------------------------------------|
| Implement cybersecurity program                   | Existing holders         | One year                                                         |
| Report whether service has commenced              | Existing holders         | One year                                                         |
| Commence service; file notification               | New grants               | One year from grant of authorization; 30 days after commencement |
| Submit cybersecurity implementation certification | New grants               | 30 days after commencement                                       |
| Submit new cross border facility notification     | Facilities-based holders | 30 days after commencement                                       |
| Submit material change notification               | All holders              | 30 days after material change                                    |
| Submit discontinuance notification and surrender  | All holders              | 30 days after three months without international service         |

## What to do now

- Inventory all authorizations, confirm a 2023 – 2024 response was filed, and consider surrendering unused or duplicative authorizations before the new deadline.
- Confirm service status under each authorization.
- Begin assembling cross-border facilities data (or wholesale provider data for resellers) and 5% ownership and control information, and review investor confidentiality commitments.
- Screen vendors and managed service providers for Covered List and foreign adversary<sup>3</sup> linkage, and lock procurement against additions of either.
- Document a written cybersecurity program consistent with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and the Cybersecurity & Infrastructure Security Agency (CISA) Cybersecurity Performance Goals (CPGs) or Center for Internet Security (CIS) Controls.
- Review adjudicated compliance history against the five character categories.
- Stand up a 30-day material change process and update discontinuance notice templates.
- Consider filing comments on the Further Notice proposals; comments will be due 30 days after Federal Register publication of the adopted item.

# New application requirements (§ 63.18(r)–(w))

These requirements would apply to applications for new authority, modification, assignment and transfer of control, and (in part) to pro forma notifications.

1. **Cross-border facilities (§ 63.18(r)).** For each cross-border facility – including data centers, points of presence (PoPs) or private interconnection points with ingress/egress switches or routers – facilities-based applicants would provide location and ownership details, IP prefixes and autonomous system numbers (ASNs), principal equipment information (including any foreign adversary or Covered List entity links), services provided, and any foreign adversary-linked physical or remote access. Resale-only applicants would identify wholesale/intermediary providers and any underlying mobile network operator (MNO). Pending applications must be amended within 30 days of any change. The information is presumptively confidential but may be shared with Team Telecom, the Department of Justice, Department of Homeland Security and Department of Defense, and reporting such facilities may trigger Team Telecom referral.
2. **Five percent ownership (§ 63.18(h)).** The disclosure threshold drops from 10% to 5% of direct or indirect equity and/or voting interests. Interests of 5%-to-under-10% held through a US publicly traded company need not be identified unless the public company has actual knowledge, measured by its share register, insider holdings, Schedules 13D/13G and Form 13F data, periodic-report beneficial ownership tables and information known “by whatever source.” The exception is limited to US publicly traded companies; there is no exception for passive or insulated interests or for private companies. The information would not be treated as presumptively confidential. The 10% foreign ownership trigger for routine Team Telecom referral is retained, but 5% information may inform the FCC’s discretion to refer any application.
3. **Services and geographic markets (§ 63.18(s)).** Applicants would disclose current and planned services, customer types, facilities versus resale and markets served. Planned information is confidential; current information is not.
4. **Third-party service providers (§ 63.18(t)).** Applicants would disclose whether they use any foreign adversary-controlled or Covered List entity, or any entity with network/ systems/communications/records access from a foreign adversary country, for managed services (“a complete, end-to-end communications solution”) supporting Section 214 operations. This is not confidential, and the FCC expects generally to refer such applications to Team Telecom. An applicant unable to confirm the information at filing must request a waiver and file status updates every 30 days.
5. **Cybersecurity certification (§ 63.18(u)).** Applicants would certify adherence to baseline cybersecurity practices structured according to an established risk management framework and incorporating an internationally recognized set of best practices. A program built on the NIST CSF incorporating CISA’s Cross-Sector Cybersecurity Performance Goals or the CIS Controls presumptively complies and, if reduced to writing, also satisfies the 5G Fund and other USF cybersecurity rules.
6. **Covered List certification (§ 63.18(v)).** Applicants would certify they will not use or add Covered List equipment or services for Section 214 service; modification, assignment and transfer applicants certify none will be added. The certification is limited to Covered List entries based on producer/provider determinations (e.g., named manufacturers and service providers) and does not reach the production location-based entries added since December 2025.
7. **Character certification (§ 63.18(w)).** Applicants would certify, as to adjudicated matters only, whether they:
  - Materially violated the Communications Act where the violation was not remediated by consent decree or compliance plan, resulted in loss of a license or authorization, or was found intentional.
  - Committed national security-related violations, including Covered List violations.
  - Made materially false statements or committed fraud concerning national security or the Communications Act.
  - Were adjudicated for such conduct by another US agency.
  - Materially breached an authorization condition, including a mitigation agreement, subject to the same three qualifiers as item (1).

Applicants would also certify service on the secretaries of defense and state and affected governors; assignors and transferors would disclose any International Signaling Point Codes (ISPCs) and whether they are part of the transaction.

# New routine conditions (§§ 63.19, 63.21)

- **Commence service within one year.** New holders must commence service within one year of grant and file a certified International Communications Filing System (ICFS) notification within 30 days of commencement identifying the date and

services; failure to commence or notify, absent a waiver, is grounds for revocation. Authorizations associated with a common carrier submarine cable instead follow the three-year cable landing license timeline. Existing holders must notify within one year of the effective date whether they have commenced service, and if not, an alternative timeframe – or surrender.

- **Permanent discontinuance.** Three consecutive months without service requires surrender and an ICFS notification within 30 days; discontinuing service without a prior waiver is grounds for revocation. Customer notices must identify the holder, date, affected areas/routes and services, and a copy must be submitted to ICFS.
- **Cross-border facility notifications.** Facilities-based holders must notify the FCC within 30 days of commencing service in any new cross-border facility or with a new underlying provider.
- **Cybersecurity.** New holders implement the program by commencement of service and certify within 30 days; existing holders implement within one year of the effective date and certify within 30 days of the effective date that they will.
- **Covered List.** New holders may not use or add Covered List equipment or services (producer/provider-based entries); existing holders may not add them, though existing equipment need not be removed.
- **Material change reporting.** All holders must notify the FCC within 30 days of a material change to previously submitted information or certifications, including changes to cross-border facilities, new 5% interest holders, new services or markets, third-party providers or certifications. OIA decides materiality.
- **Enforcement.** Noncompliance with any reporting requirement is grounds for revocation and/or termination, and the FCC may review any authorization at any time.

## One-time information collection

Every existing holder would file the same cross-border facilities, ownership, services/markets, third-party provider, cybersecurity, Covered List, and character disclosures and certifications described above, plus a list of all its authorizations explaining why it needs more than one. The FCC “strongly encourage[s]” surrendering duplicative authorizations; holders that surrender everything before the deadline need not respond. Information must be current as of 30 days before filing; the deadline is no fewer than 30 days after the collection’s effective date. Holders certify accuracy under a “substantial due diligence” (not strict liability) standard; noncompliance exposes holders to forfeitures and revocation.

## Revocation of 2023 – 2024 nonresponders

Holders that did not respond to the 2023 Evolving Risks Order collection would be presumed to be no longer operating. OIA would publish a Federal Register list giving holders 30 days to respond or surrender, then 15 more days before revocation. Late responders are not subject to these procedures. Reinstatement nunc pro tunc could be sought within six months on good cause.

## Further Notice proposals

None of the following is adopted; each would require a further order.

- **Presumptive disqualifying conditions (proposed § 63.27).** Applicants that are foreign adversary-controlled, on the Covered List, or previously denied or revoked on national security grounds (and the affiliates and subsidiaries of any such revoked or denied entity); applicants with foreign adversary financing, strategic partnerships or mergers affecting Section 214 operations; and applicants with foreign adversary-linked senior officials – rebuttable only by clear and convincing evidence.
- **Indefeasible right of use (IRU), capacity lease, dark fiber and spectrum arrangements.** A proposed condition barring new or extended arrangements giving foreign adversary-controlled, Covered List or previously revoked entities ownership, control, management authority or meaningful operational control over a holder’s network; contractual flow-down to customers and downstream customers; a filing within 60 days of commencing service and annually listing all such arrangements with copies of the agreements (confidential); and a one-time certification from existing holders within 60 days.
- **Foreign adversary-produced equipment and services.** No use by new applicants, and no addition by any holder, of equipment or services “produced (including any major stage of the process ... including manufacturing, assembly, design, and development) or provided by” foreign adversary-controlled or Covered List entities; existing holders would certify current use within 60 days.
- **Third-party service providers.** A prohibition on foreign adversary-linked providers under a broadened definition reaching

any third party whose services – including network operations center (NOC), maintenance, billing, customer support, security, IT, cloud and data center services – could give it access to principal equipment, domestic communications, lawful US process or customer records.

- **Cyber and physical security risk management plans** signed by a senior officer and producible on request, with two-year record retention; **incident reporting** within 72 (or 48) hours; and mandatory **cyber hygiene** measures.
- **Other:** prohibiting access by foreign adversary-linked personnel; disclosing all facility locations; prior approval before serving a foreign adversary country; concurrent Team Telecom filings for mitigation-agreement holders; codified modification rules (§ 63.26); and broad interagency information sharing (§ 63.30).

#### Notes

1. Review of International Section 214 Authorizations to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks; Amendment of the Schedule of Application Fees Set Forth in Sections 1.1102 through 1.1109 of the Commission’s Rules, IB Docket No. 23-119, MD Docket No. 23-134, Report and Order and Further Notice of Proposed Rulemaking, FCC-CIRC 2610-05 (circulated Oct. 8, 2026) (Draft Order). The document “has been circulated for tentative consideration by the Commission at its October 29, 2026, open meeting,” remains “subject to change,” and “does not constitute any official action by the Commission.” Id. at 1 n.\*.
2. 47 CFR § 1.1203(a)–(b); Draft Order at 1 n.\* (Sunshine Agenda “is typically released a week prior to the Commission’s meeting”). The FCC released the tentative agenda for the October 29, 2026, open meeting on October 8, 2026; as of October 21, 2026, no Sunshine notice had been released.
3. “Foreign adversary,” “foreign adversary country” and “owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary” are defined in 47 CFR § 1.70001(e)–(g) by reference to the Department of Commerce’s determinations in 15 CFR § 791.4. Currently, the following are identified as foreign adversaries: China (including the Hong Kong and Macau Special Administrative Regions), Cuba, Iran, North Korea, Russia and the Maduro Regime. 15 CFR § 791.4(a).

If you would like to discuss these requirements, prepare for the one-time collection or participate in the comment process, please contact one of the Cooley lawyers listed below.

This alert is based solely on the circulated draft of FCC-CIRC 2610-05 released October 8, 2026, which remains subject to change before FCC’s October 29, 2026, vote.

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as “Cooley”). By accessing this content, you agree that the information provided does not constitute legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction, and you should not act or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. When advising companies, our attorney-client relationship is with the company, not with any individual. This content may have been generated with the assistance of artificial intelligence (AI) in accordance with our AI Principles, may be considered Attorney Advertising and is subject to our [legal notices](#).

## Key Contacts

|                                      |                                          |
|--------------------------------------|------------------------------------------|
| Brett P. Ferenchak<br>Washington, DC | bferenchak@cooley.com<br>+1 202 776 2138 |
| Tamar E. Finn<br>Washington, DC      | tfinn@cooley.com<br>+1 202 728 7129      |

|                                       |                                            |
|---------------------------------------|--------------------------------------------|
| Ronald W. Del Sesto<br>Washington, DC | rdelsesto@cooley.com<br>+1 202 728 7128    |
| J.G. Harrington<br>Washington, DC     | jgharrington@cooley.com<br>+1 202 776 2818 |

This information is a general description of the law; it is not intended to provide specific legal advice nor is it intended to create an attorney-client relationship with Cooley LLP. Before taking any action on this information you should seek professional counsel.

Copyright © 2023 Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304; Cooley (UK) LLP, 22 Bishopsgate, London, UK EC2N 4BQ. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Cooley LLP as the author. All other rights reserved.