Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Digitalsystem Technology Inc.	)	ITC-214-20240326-00054
	)	
Application for Global Facilities-Based and Global Resale International Telecommunications Authority Pursuant to Section 214 of the Communications Act of 1934, as Amended	)	

MEMORANDUM OPINION AND ORDER

Adopted: June 30, 2026 **Released: July 7, 2026**

By the Commission:

TABLE OF CONTENTS

I. INTRODUCTION

1. In this Memorandum Opinion and Order (Order), we deny Digitalsystem Technology Inc.'s (Digitalsystem) application for an international section 214 authorization to provide international

telecommunications services between the United States and foreign destinations.[1] First, based on our public interest analysis under section 214 of the Communications Act of 1934, as amended (Act),[2] and solely on the totality of the extensive unclassified record evidence, including the filing submitted by the Executive Branch agencies in the record,[3] we find that grant of Digitalsystem's application would result in substantial and significant risks to national security and law enforcement that cannot be addressed through a mitigation agreement. Importantly, we agree with the Executive Branch agencies[4] that Digitalsystem is subject to the jurisdiction and control[5] of the government of China, and Digitalsystem's related partnerships and planned operations raise significant national security and law enforcement concerns.[6] Second, based on the evidence in the record, we further agree with the Executive Branch agencies that there is significant risk that the government of China and other threat actors could exploit any vulnerabilities to the detriment of U.S. national security and law enforcement interests. Third, we find that the Commission and the Executive Branch agencies cannot trust or rely on Digitalsystem to adhere to mitigation measures, and therefore that the national security and law enforcement risks cannot be addressed through mitigation. Finally, although it is not necessary to support these findings and conclusions, we find that the classified evidence submitted by the Committee further supports our

[1] Application of Digitalsystem Technology Inc. for International Section 214 Authority, File No. ITC-214-20240326-00054 (filed Mar. 26, 2024), https://fccprod.servicenowservices.com/icfs?id=ibfs_application_summary&number=ITC-214-20240326-00054 (Digitalsystem Application); 47 U.S.C. § 214.

[2] 47 U.S.C. § 214.

[3] Recommendation of the Committee for the Assessment of Foreign Participation in the U.S. Telecommunications Services Sector to Deny the Application, File No. ITC-214-20240326-00054 (filed Apr. 2, 2026) (filing a redacted version); Recommendation of the Committee for the Assessment of Foreign Participation in the U.S. Telecommunications Services Sector to Deny the Application, File No. ITC-214-20240326-00054 (filed Apr. 7, 2026) (filing a business confidential version). We refer hereafter to the public redacted and business confidential filings collectively as the Committee Recommendation. *See infra* note 4. We conclude that the publicly-available information and the applicant's confidential business information provided by the Executive Branch agencies, alone, is sufficient to support our findings and decision in this *Order*. The applicant has access to the applicant's own business confidential information and the extent to which the Committee has relied on the applicant's information in its Recommendation. As we note herein, the applicant does not dispute the salient facts discussed in the Committee Recommendation. We also note there is a classified section that discusses how the classified information provided to the Commission by the Executive Branch agencies further supports the findings and decision in this *Order*. *See infra* para. 53; 47 U.S.C. 154(j); *Use of Classified Information; Policy to be Followed in Future Licensing of Facilities for Overseas Communications*, Order, FCC 78-755, 44 Rad. Reg. 2d 607, 611, para. 10 (1978).

[4] For purposes of this filing, the Executive Branch agencies include the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Committee). Committee Recommendation at 1 & n.1 ("This filing is made in coordination with Committee Advisors in accordance with subsections 3(d) and 9(f) of Executive Order 13913."); Executive Order No. 13913 of April 4, 2020, Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, 85 Fed. Reg. 19643, 19643 (Apr. 8, 2020) (Executive Order 13913); *see infra* para. 3 (discussing the Committee).

[5] We use the terms "jurisdiction" and "control" in this *Order* given the use of this terminology in the Committee Recommendation and in light of our findings, as discussed below, that China has jurisdiction over Digitalsystem's majority owner, an individual who is a citizen of China and holds 70% ownership and therefore majority control of Digitalsystem. *See infra* section III.b.1; *see, e.g.*, 47 CFR § 63.09(b) ("Control includes actual working control in whatever manner exercised and is not limited to majority stock ownership. Control also includes direct or indirect control, such as through intervening subsidiaries.") (emphasis omitted); 47 CFR § 63.24, Note to paragraph (d); 47 CFR § 1.70001(g)(4). By using these terms, and based on the record, we intend to capture these direct and indirect relationships by which Digitalsystem is under the control and influence of the government of China, which we discuss further herein.

[6] *See* Committee Recommendation at 19.

decisions here. Accordingly, we find that the present and future public interest, convenience, and necessity would not be served by the grant of international section 214 authority to Digitalsystem.[7]

II. BACKGROUND

A. International Section 214 Applications

2. Section 214(a) of the Act requires a carrier to obtain Commission authorization before constructing, acquiring, or operating any line, and prior to engaging in transmission through any such line.[8] Applicants seeking to provide U.S.-international common carrier telecommunications service (also referred to herein as U.S.-international "telecommunications service")[9] must file an application for international 214 authority,[10] which requires a showing that a grant of the application will serve the public interest.[11]

3. As part of the Commission's public interest analysis, the Commission considers a number of factors and examines the totality of the circumstances of each particular situation.[12] One of the factors

[7] 47 CFR § 63.18.

[8] 47 U.S.C. § 214(a); *see Reform of Rules and Policies on Foreign Carrier Entry Into the U.S. Telecommunications Market*, IB Docket No. 12-299, Report and Order, 29 FCC Rcd 4256, para. 2, n.2 (2014) (*2014 Foreign Carrier Entry Order*) ("Any party seeking to provide common carrier telecommunications services between the United States, its territories or possessions, and a foreign point must request authority by application pursuant to section 214(a) of the Act, 47 U.S.C. § 214(a), and section 63.18 of the Commission's rules, 47 C.F.R. § 63.18."). The Supreme Court has determined that the Commission has considerable discretion in deciding how to make its section 214 public interest findings. *FCC v. RCA Communications, Inc.*, 346 U.S. 86, 90 (1953); *see Policy and Rules Concerning Rates for Competitive Common Carrier Services and Facilities Authorizations Therefor*, CC Docket No. 79-252, First Report and Order, 85 FCC 2d 1, 40-44, paras. 117-29 (1980) (discussing the Commission's authority under section 214(a) of the Act); *Streamlining the International Section 214 Authorization Process and Tariff Requirements*, IB Docket No. 95-118, Notice of Proposed Rulemaking, 10 FCC Rcd 13477, 13480, para. 6 (1995) (*1995 Streamlining NPRM*); *Streamlining the International Section 214 Authorization Process and Tariff Requirements*, IB Docket No. 95-118, Report and Order, 11 FCC Rcd 12884, 12903, para. 44, n.63 (1996) (*1996 Streamlining Order*); Telecommunications Act of 1996, Pub. L. 104-104, § 402(b)(2)(A) (1996), codified at 47 U.S.C. § 214 nt. ("The Commission shall permit any common carrier—(A) to be exempt from the requirements of section 214 of the Communications Act of 1934 for the extension of any line; . . .").

[9] *See* 47 U.S.C. § 153(50) ("The term 'telecommunications' means the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received."); *id.* § 153(53) ("The term 'telecommunications service' means the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used.").

[10] *See* 47 CFR § 63.18 ("Except as otherwise provided in this part, any party seeking authority pursuant to Section 214 of the Communications Act of 1934, as amended, to construct a new line, or acquire or operate any line, or engage in transmission over or by means of such additional line for the provision of common carrier communications services between the United States, its territories or possessions, and a foreign point shall request such authority by formal application. The application shall include information demonstrating how the grant of the application will serve the public interest, convenience, and necessity. Such demonstration shall consist of the following information, as applicable . . . .").

[11] 47 CFR § 63.18.

[12] *Rules and Policies on Foreign Participation in the U.S. Telecommunications Market; Market Entry and Regulation of Foreign-Affiliated Entities*, IB Docket Nos. 97-142 and 95-22, Report and Order and Order on Reconsideration, 12 FCC Rcd 23891, 23918-21, paras. 59-66 (1997) (*Foreign Participation Order*), recon. denied, 15 FCC Rcd 18158 (2000); *Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership*, IB Docket No. 16-155, Notice of Proposed Rulemaking, 31 FCC Rcd 7456 (2016) (*Executive Branch Process Reform NPRM*); *Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership*, Report and Order, 35 FCC Rcd 10927, 10963-64, para. 92 (2020) (*Executive Branch Process Reform Report and Order*); *see, e.g.*, *China Mobile International (USA) Inc.*;

(continued….)

the Commission considers is whether the application for the authorization raises any national security, law enforcement, foreign policy, or trade policy concerns related to the applicant's reportable foreign ownership.[13] With regard to this factor, for nearly 30 years, the Commission has sought the expertise of the relevant Executive Branch agencies and has accorded deference to their expertise in identifying such a concern.[14] The Commission has formalized the review process for the Executive Branch agencies to complete their review consistent with Executive Order No. 13913 dated April 4, 2020, that established the Committee.[15] As part of that process, the Commission refers applications with reportable foreign ownership to the Committee for it to assess national security and law enforcement concerns.[16] Following its review, the Committee may recommend to the Commission that the Commission grant the application contingent on mitigation measures; recommend that the Commission deny the application due to the risk to the national security or law enforcement interests of the United States; or state that it has no recommendation and no objection to the Commission's granting the application.[17] The Commission ultimately makes an independent decision in light of all of the information in the record, including any information provided by the applicant, authorization holder, or licensee in response to any filings by the

Application for Global Facilities-Based and Global Resale International Telecommunications Authority Pursuant to Section 214 of the Communications Act of 1934, as Amended, Memorandum Opinion and Order, 34 FCC Rcd 3361 (2019) (*China Mobile USA Order*).

[13] Foreign Participation Order, 12 FCC Rcd at 23918-21, paras. 59-66; Executive Branch Process Reform Report and Order, 35 FCC Rcd at 10963-64, para. 92.

[14] *Foreign Participation Order*, 12 FCC Rcd at 23918-21, paras. 59-66. In the 1997 *Foreign Participation Order*, the Commission affirmed its previously *ad hoc* policy of seeking Executive Branch input on any national security, law enforcement, foreign policy, or trade policy concerns related to the reportable foreign ownership as part of its overall public interest review of an application. *Id.*

[15] Executive Order No. 13913 of April 4, 2020, Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, 85 Fed. Reg. 19643, sec. 1 (stating that, "[t]he security, integrity, and availability of United States telecommunications networks are vital to United States national security and law enforcement interests"); *id.* at 19643-44 (establishing the "Committee," composed of the Secretary of Defense (DOD), the Secretary of Homeland Security (DHS), and the Attorney General of the Department of Justice (DOJ), who serves as the Chair, and the head of any other executive department or agency, or any Assistant to the President, as the President determines appropriate (Members), and also providing for Advisors, including the Secretary of State, the Secretary of Commerce, and the United States Trade Representative (USTR)).

[16] The Commission's rules allow for either streamlined or non-streamlined processing of applications for international section 214 authority or modification, assignment, or transfer of control of international section 214 authority. *See* 47 CFR § 63.12. If an applicant has reportable foreign ownership, the application process usually is not streamlined and the Office of International Affairs (OIA) refers the application to Executive Branch agencies for review at the time it places the application on "Accepted for Filing" public notice. *Executive Branch Process Reform Order*, 35 FCC Rcd at 10928-31, 10957-58, paras. 3-7, 81; *2016 Executive Branch Process Reform NPRM*, 31 FCC Rcd at 7471, para. 38; 47 CFR § 1.40001. Under our rules and procedures, applicants with reportable foreign ownership are required to submit answers to a set of standardized national security and law enforcement questions to the Committee at the time the applicant files its application with the Commission. *Executive Branch Process Reform Order*, 35 FCC Rcd at 10935, para. 18; *see generally* 47 CFR § 1.40003 (listing the categories of information an applicant, petitioner, and/or other filer subject to referral must provide to the Executive Branch agencies); *see Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership, Second Report and Order*, 36 FCC Rcd 14848, 14883-14966, Attachs. A-G (*2021 Standard Questions Order*).

[17] 47 CFR § 1.40004(b)(1)-(3), (c)(2)(i)-(iii); Executive Order 13913, 85 Fed. Reg. at 19646, sec. 9(a). The Committee has 120 days for its initial review, and an additional 90 days for its secondary assessment if the Committee determines that the risk to national security or law enforcement interests cannot be mitigated with standard mitigation measures. 47 CFR § 1.40004(b)-(c).

Executive Branch agencies.[18] This holistic review, which gives all affected entities due process, is very different than the government of China's categorical restriction on foreign-controlled companies operating Basic Telecommunications Services, China's functional equivalent of a section 214 authorization.[19]

B. Digitalsystem Technology Inc.'s Application

4. Digitalsystem is a California corporation that is controlled and majority-owned by a citizen of China.[20] Specifically, Digitalsystem is 70% owned by Hui Xie (a citizen of China) and 30% owned by Yi Zhou (a U.S. citizen).[21] Based on information in the record, Hui Xie is {[ ]}[22] and is the Chief Executive Officer (CEO)[23] and {[ ]} of Digitalsystem.[24] Yi Zhou is {[ ]}[25] Digitalsystem's website indicates that it "is a trusted IT solutions provider headquartered in the heart of Los Angeles, serving businesses globally with a strong presence across Mexico, Brazil, Hong Kong, and China."[26] Digitalsystem's website adds that, "[w]ith strategically located Points of Presence (POPs) across these regions, we deliver high-speed connectivity and global IDC solutions that ensure reliable, low-latency services wherever our clients operate."[27] Digitalsystem offers services such as "Data Center Management,"[28] "Network & Low-Voltage Implementation,"[29] Cloud Migration & DevOps Automation,"[30] "Zero Trust Architecture,"[31] and "Disaster Recovery &

---

[18] *Foreign Participation Order*, 12 FCC Rcd at 23921, para. 66 ("We emphasize that the Commission will make an independent decision on applications to be considered and will evaluate concerns raised by the Executive Branch agencies in light of all the issues raised (and comments in response) in the context of a particular application.").

[19] *See Special Administrative Measures for Foreign Investment Access* (Negative List) (2024 Edition) (promulgated by the Nat. Dev. & Reform Comm. & Ministry of Commerce, Sept. 8, 2024, effective Nov. 1, 2024) (China).

[20] Digitalsystem Application, Attach. 2 at 1.

[21] *Id.*

[22] Committee Recommendation at 5. Material that is set off by double brackets {[ ]} is subject to confidential treatment under the Commission's rules and is redacted from the public version of this document.

[23] Digitalsystem Application, FCC Form 214 at 5. Digitalsystem's application identified "Hui Xie" as the CEO in the certification and "Alan Xie" as a point of contact for the application. Digitalsystem Application, FCC Form 214 at 1, 5. However, Digitalsystem did not indicate in the application that {[ ]}

[24] Committee Recommendation at 5.

[25] Committee Recommendation at 5 ({[ ]}). According to the record, Hui Xie and Yi Zhou {[ ]} Committee Recommendation at 5 ({[ ]})

[26] Digitalsystem Technology Inc., *About Us—Company Overview*, https://www.digitalsystem.net/about.html?i=0 (last visited June 17, 2026) (*Digitalsystem Company Overview*); *see* Committee Recommendation at 6, 25, 28 (identifying Digitalsystem's public website).

[27] *Digitalsystem Company Overview*.

[28] Digitalsystem Technology Inc., *Managed IT & Infrastructure—Data Center Management*, https://www.digitalsystem.net/services/data_center_management.html (last visited June 12, 2026).

[29] Digitalsystem Technology Inc., *Managed IT & Infrastructure—Network & Low-Voltage Implementation*, https://www.digitalsystem.net/services/network.html (last visited June 12, 2026).

[30] Digitalsystem Technology Inc., *Cloud & DevOps—Cloud Migration & DevOps Automation*, https://www.digitalsystem.net/services/cloud_migration.html (last visited June 12, 2026).

[31] Digitalsystem Technology Inc., *Cybersecurity & Compliance—Zero Trust Architecture*, https://www.digitalsystem.net/services/zero_trust_architecture.html (last visited June 12, 2026).

Business Continuity,"[32] and the industries include manufacturing, logistics and transportation, financial services, healthcare, and energy and utilities.[33]

5. On March 26, 2024, Digitalsystem filed an application with the Commission requesting authority under section 214 of the Act and section 63.18 of the Commission's rules to provide global or limited global facilities-based service and resale service.[34] Digitalsystem seeks to provide international telecommunications services to all international points,[35] {[ ]}[36] On June 14, 2024, OIA released a public notice finding Digitalsystem's international section 214 application acceptable for filing and placing the application on non-streamlined processing.[37] At the same time, OIA referred the application to the relevant Executive Branch agencies, including the Committee,[38] and the Committee notified the Commission that it was reviewing the application for any national security and law enforcement issues and requested that the Commission defer action on the application until the Committee completed its review.[39]

6. On April 2, 2026, after its initial review and a secondary assessment,[40] the National Telecommunications and Information Administration (NTIA), on behalf of the Committee, filed a recommendation to deny the application.[41] The Committee recommends that the Commission deny the application "because Digitalsystem's application presents risks to the national security and law enforcement interests of the United States[.]"[42] The Committee states that "[t]hese risks are posed in part by the government of [China], which presents significant threats within the context of this application."[43] Furthermore, the Committee states that the risks presented by the application cannot be adequately mitigated due to {[ ]}[44] in

[32] Digitalsystem Technology Inc., *Cybersecurity & Compliance—Disaster Recovery & Business Continuity*, https://www.digitalsystem.net/services/disaster_recovery.html (last visited June 12, 2026).

[33] Digitalsystem Technology Inc., https://www.digitalsystem.net/ (last visited June 12, 2026) (identifying categories under the "Industries" tab).

[34] Digitalsystem Application, FCC Form 214 at 2.

[35] Digitalsystem Application, FCC Form 214 at 3.

[36] Committee Recommendation at 6 ({[ ]}).

[37] *Non Streamlined International Applications/Petitions Accepted For Filing*; *Section 214 Applications (47 CFR §§ 63.18, 63.24); Section 310(b) Petitions (47 CFR § 1.5000)*, File No. ITC-214-20240326-00054, Public Notice, Report No. TEL-02369NS, 2024 WL 3042721 (OIA rel. June 14, 2024).

[38] *Id.*

[39] *Non Streamlined International Applications/Petitions Accepted For Filing*; *Section 214 Applications (47 CFR §§ 63.18, 63.24); Section 310(b) Petitions (47 CFR § 1.5000)*, File No. ITC-214-20240326-00054, Public Notice, Report No. TEL-02373NS, 2024 WL 3249590 (OIA rel. June 28, 2024).

[40] *See supra* note 17.

[41] *See generally* Committee Recommendation; *Non Streamlined International Applications/Petitions Accepted For Filing*; *Section 214 Applications (47 CFR §§ 63.18, 63.24); Section 310(b) Petitions (47 CFR § 1.5000)*, File No. ITC-214-20240326-00054, Public Notice, Report No. TEL-02640NS, 2026 WL 1078976 (OIA Apr. 10, 2026).

[42] Committee Recommendation at 1.

[43] Committee Recommendation at 1.

[44] Committee Recommendation at 2.

addition to Digitalsystem's "conflicting, incomplete, and/or misleading responses" to the Committee "which raise doubts about Digitalsystem's truthfulness and ability to engage in a productive compliance relationship."[45]

7. On April 13, 2026, OIA issued a letter providing an opportunity for Digitalsystem to file an Opposition to the Committee Recommendation.[46] On May 7, 2026, Digitalsystem filed an Opposition to the Committee Recommendation.[47]

III. DISCUSSION

8. Applying our public interest analysis under section 214 of the Act and based solely on the totality of the extensive unclassified record evidence alone, including the filing submitted by the Executive Branch agencies in the record, we find that the present and future public interest, convenience, and necessity would not be served by the grant of international section 214 authority to Digitalsystem,[48] and we deny the application. We find that Digitalsystem, through its control and majority ownership by Hui Xie, a citizen of China, is subject to the jurisdiction and control of the government of China, which is identified as a foreign adversary by the Committee[49] and the Commission.[50] We find that Digitalsystem's partnerships with a Hong Kong affiliate and other entities and its planned operations raise significant national security and law enforcement concerns. Based on the evidence in the record, we find there is significant risk that the government of China and other threat actors could exploit these vulnerabilities to the detriment of U.S. national security and law enforcement interests. We find that the Commission and the Committee cannot trust or rely on Digitalsystem to adhere to mitigation measures, and that the national security and law enforcement risks cannot be addressed through mitigation with the Committee. Additionally, although it is not necessary to support these findings and conclusions, we find that the classified evidence submitted by the Committee further supports our decisions here.

A. Standard of Review

9. Under section 214 of the Act and section 63.18 of the Commission's rules, as well as longstanding Commission precedent, Digitalsystem must demonstrate how grant of its international section 214 application would serve the public interest, convenience, and necessity and the Commission must find that the grant of the application will serve these purposes.[51] As part of the Commission's public interest analysis, the Commission considers whether such an application raises national security, law enforcement, foreign policy, or trade policy concerns related to the applicant's reportable foreign

[45] Committee Recommendation at 2.

[46] Letter from Denise Coca, Chief, Telecommunications and Analysis Division, FCC Office of International Affairs, to Hui Xie, CEO, Digitalsystem Technology Inc, et al., at 1-2 (OIA Apr. 13, 2026), DA 26-357 (on file in File No. ITC-214-20240326-00054) (Digitalsystem Letter) ("Digitalsystem may file an Opposition to the Committee Recommendation no later than Wednesday, May 13, 2026. The Opposition should be filed electronically in File No. ITC-214- 20240326-00054 via ICFS. The Opposition must also be served on the Committee. The Committee will have until Friday, June 12, 2026, to file a Reply to the Opposition.").

[47] Digitalsystem Technology Inc., Opposition to the Recommendation of the Committee for the Assessment of Foreign Participation in the U.S. Telecommunications Services Sector to Deny the Application, File No. ITC-214-20240326-00054 (filed May 7, 2026), https://fccprod.servicenowservices.com/icfs?id=ibfs_application_summary&number=ITC-214-20240326-00054 (Digitalsystem Opposition). Although the Digitalsystem Opposition is dated "May 13, 2026" on pages five and six of the document, this document was actually filed six days prior on May 7, 2026.

[48] 47 U.S.C. § 214; 47 CFR § 63.18.

[49] *See generally* Committee Recommendation.

[50] *See infra* para. 15.

[51] 47 U.S.C. § 214; 47 CFR § 63.18; *Foreign Participation Order*, 12 FCC Rcd at 23920-21, para. 65; *China Mobile USA Order*, 34 FCC Rcd at 3367, para. 11.

ownership.[52] As the Commission has stated, an applicant for section 214 authority is entitled to a rebuttable presumption that grant of the application is in the public interest on competition grounds; "[h]owever, no such presumption applies to national security and law enforcement concerns, which are separate, independent factors the Commission considers in its public interest analysis."[53]

B. Denial of Section 214 Application

1. Digitalsystem, Through its Control and Majority Ownership by a Citizen of China, is Subject to the Government of China's Jurisdiction and Control

10. The record evidence shows that Digitalsystem, through its control and majority ownership by a citizen of China,[54] is subject to the government of China's jurisdiction and control. The Committee states that Hui Xie, as a citizen of China, is subject to the government of China's jurisdiction, including laws of China that "provide[] PRC intelligence services with the power to compel Chinese citizens and organizations 'to cooperate, assist, and support Chinese intelligence efforts *wherever they are in the world*.'"[55] The Committee asserts that "Xie and Digitalsystem have several jurisdictional hooks to PRC and Hong Kong which may mean they could be directly, formally compelled to act by Chinese and Hong Kong entities"[56] and that the government of China exerts {[ ]}[57] The Committee states that the government of China, through laws such as the 2017 National Intelligence Law, could compel Hui Xie "to cooperate, assist, and support Chinese intelligence efforts, even though he resides in the United States."[58] The Committee explains that the government of China uses comprehensive laws—including the 2015 National Security Law,[59] 2017 Cybersecurity Law,[60]

[52] *See Foreign Participation Order*, 12 FCC Rcd at 23918-21, paras. 59-66; *Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership*, Report and Order, 35 FCC Rcd 10927, 10963-64, para. 92 (2020).

[53] *China Mobile USA Order*, 34 FCC Rcd at 3367, para. 11 (citing *Foreign Participation Order*, 12 FCC Rcd at 23920-21, para. 65).

[54] Digitalsystem Application, Attach. 2 at 1; *see supra* note 5.

[55] Committee Recommendation at 18 ("Xie is a citizen of the PRC, meaning the PRC has jurisdiction over him and could compel him to cooperate, assist, and support Chinese intelligence efforts, even though he resides in the United States.").

[56] Committee Recommendation at 18.

[57] Committee Recommendation at 2.

[58] Committee Recommendation at 18.

[59] Committee Recommendation at 10 & n.45 ("[T]he PRC's 2015 National Security Law 'imposes broad obligations on corporations as well as citizens to assist and cooperate with the Chinese government in protecting what it defines as national security,' which is itself broadly defined, including the duty to 'promptly report any clues and provide evidence of any activities endangering national security and to assist military agencies and relevant departments with national security efforts.'") (quoting *In Camera, Ex Parte* Classified Decl. of David Newman, Principal Deputy Assistant Att'y Gen., Nat'l Sec. Div., U.S. Dep't of Just., Doc. No. 2066897 at Gov't App. 51 para. 19, *TikTok Inc.* v. *Garland,* Case Nos. 24-1113, 24-1130, 24-1183 (D.C. Cir. July 26, 2024) (publicly filed redacted version) (Newman Decl.)).

[60] Committee Recommendation at 10 & n.46-47 ("The PRC's 2017 Cybersecurity Law similarly requires Chinese companies (including those that construct, operate, maintain, and use networks) to 'store their data within China,' 'cooperate with crime and security investigations,' and 'allow full access to data to Chinese authorities.' PRC citizens or companies that oppose requests from PRC intelligence or security services do not have adequate legal recourse to challenge such requests.") (citing Dr. Christopher Ashely Ford, Assistant Sec'y of State, U.S. Dep't of State Bureau of Int'l Security and Nonproliferation, Remarks at the Multilateral Action on Sensitive Technologies Conference (Sept. 11, 2019), https://web.archive.org/web/20210105011801/https://www.state.gov/huawei-and-its-siblings-the-chinese-tech-giants-national-security-and-foreign-policy-implications).

2017 National Intelligence Law,[61] and 2014 Counter-Espionage Law[62]—to "'effectively blur[] the line between the private and public sector,'" such that "'Chinese companies lack meaningful independence from the PRC's agenda and objectives.'"[63] Among other things, the Committee explains that the government of China has revised the 2014 Counter-Espionage Law to explicitly require "'[a]ll citizens and organizations' to 'support and assist in counter-espionage work.'"[64] In addition, the Committee states that Hui Xie, a citizen of China, {[

]}[65] Further, the Committee states that {[

]}[67] Based on the Committee Recommendation, {[ ]} amplify the possibility that Digitalsystem or its majority owner will be forced to comply with the government of China's requests without sufficient legal procedures subject to independent judicial oversight.

11. Digitalsystem does not dispute that the company and its majority owner, a citizen of

[61] Committee Recommendation at 11 & n.48-49 ("The PRC's 2017 National Intelligence Law similarly authorizes 'national intelligence work agencies' to use 'any "necessary methods, means, and channels"' to carry out 'intelligence work both domestically and abroad,' including by establishing 'cooperative relationships with relevant individuals and organizations' and 'entrust[ing] them with related tasks.'") (quoting Newman Decl. at para. 22).

[62] Committee Recommendation at 11 ("The PRC's 2014 Counter-Espionage Law further increases the PRC government's access to ostensibly private facilities and data; for example it authorizes 'national security agency staff' to 'enter restricted areas, locations, and units,' and to 'inspect the electronic devices, facilities, and relevant procedures and tools of concerned individuals and organizations,' and requires citizens and organizations to 'support and assist' such efforts.") (quoting Newman Decl. at para. 23).

[63] Committee Recommendation at 11 (quoting Newman Decl. at paras. 25, 17). In addition to these laws, the Committee explains that a group of laws passed in 2020 and 2021—such as the Cyber Vulnerability Reporting Law and its implementing regulations, Personal Information Protection Law, Anti-Foreign Sanctions Law, Data Security Law—also increase the threat from the government of China. *Id.* at 11-12. According to the Committee, "for example, the PRC's 2020 Data Security Law, in effect 2021, expands the PRC government's access to, and control of, companies and data within the PRC and subjects cross-border data flows to additional regulatory requirements and prohibitions." *Id.* (citations omitted). Additionally, the Committee observes that the Cyber Vulnerability Reporting Law and implementing regulations "require any business operating in the PRC to report software vulnerabilities to [the Ministry of Industry and Information Technology] within forty-eight hours of their discovery," and "prohibit researchers from: 'publishing information about vulnerabilities before a patch is available, unless they coordinate with the product owner and the [Ministry of Industry and Information Technology]; publishing proof-of-concept code used to show how to exploit a vulnerability; and exaggerating the severity of a vulnerability.'" *Id.* at 12 (citations omitted). The Committee notes that "[i]n effect, the regulations push all software-vulnerability reports" to the Ministry of Industry and Information Technology "before a patch is available." *Id.* These laws provided the government of China with more access to information about potential software vulnerabilities just as there was "a corresponding uptick in the number of zero-day vulnerabilities deployed by PRC-based hacking group," with Microsoft's Digital Defense Report in 2022 finding the increase "likely" due to these regulations. *See id.* at 12 (citing Microsoft's Digital Defense Report 2022 at 39); Microsoft, Microsoft Digital Defense Report 2022 (2022), https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/microsoft-digital-defense-report-2022.pdf?culture=en-us&country=us.

[64] Committee Recommendation at 12-13 & n.57-59 (quoting Newman Decl., Ex. E, Art. 8).

[65] Committee Recommendation at 18.

[66] Committee Recommendation at 18.

[67] Committee Recommendation at 18.

China, are subject to the government of China's jurisdiction and the laws of the government of China.[68] Instead, Digitalsystem contends that "[c]itizenship alone has never been a per se disqualifying factor for Section 214 authority."[69] Digitalsystem further states that "Mr. Xie has resided in the United States for years, has no history of noncompliance with U.S. law, and—as set forth below—commits to never accessing U.S. core systems from mainland China and to submitting to independent security oversight."[70] We find these contentions unpersuasive.

12. We agree with the Committee that Digitalsystem and its majority owner, Hui Xie, a citizen of China, are subject to the jurisdiction of the government of China and consequently the laws of China, and that Digitalsystem is under the government of China's control and influence.[71] Our determination here is consistent with the Commission's prior findings that the government of China's 2017 National Intelligence Law requires that "'[a]ll organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national intelligence work secrets they are aware of.'"[72] Moreover, the Commission has found unpersuasive the contention that the government of China construes or would construe "lawful rights and interests of individuals and organizations" in favor of U.S. law to whatever extent the 2017 National Intelligence Law and any actions directed or undertaken pursuant to that law conflicts with U.S. law.[73] Further, as the Commission has stated in prior proceedings, the combination of the government of China's cybersecurity and national intelligence laws presents serious and substantial national security and law enforcement concerns,[74] and

[68] *See* Digitalsystem Opposition at 2.

[69] Digitalsystem Opposition at 2.

[70] Digitalsystem Opposition at 2.

[71] *See* Committee Recommendation at 2, 18.

[72] *Pacific Networks Corp. and ComNet (USA) LLC*, GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199, Order on Revocation and Termination, 37 FCC Rcd 4220, 4278, para. 68 (2022) (*Pacific Networks/ComNet Order on Revocation and Termination*), *aff'd*, *Pac. Networks Corp. v. FCC*, 77 F.4th 1160 (D.C. Cir. 2023) (citing 2017 National Intelligence Law, Article 7); *see China Mobile USA Order*, 34 FCC Rcd at 3369, para. 17 ("For example, Article 7 of the 2017 National Intelligence Law provides that '[a]n organization or citizen shall support, assist in and cooperate in national intelligence work in accordance with the law and keep confidential the national intelligence work that it or he knows.'"); *China Telecom (Americas) Corporation*, GN Docket No. 20-109, File Nos. ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285, Order on Revocation and Termination, 36 FCC Rcd 15966, 16006, para. 63 (2021) (*China Telecom Americas Order on Revocation and Termination*), *aff'd*, *China Telecom (Americas) Corp. v. FCC*, 57 F.4th 256 (D.C. Cir. 2022); *China Unicom (Americas) Operations Limited*, GN Docket No. 20-110, File Nos. ITC-214-20020728-00361, ITC-214-20020724-00427, Order on Revocation, 37 FCC Rcd 1480, 1521-22, paras. 64-65 (2022) (*China Unicom Americas Order on Revocation*), *aff'd*, *China Unicom (Americas) Operations Ltd. v. FCC*, 124 F.4th 1128 (9th Cir. 2024). In the *China Mobile USA Order*, the Commission further discussed that "Article 14 permits Chinese intelligence institutions to request citizens and organizations to provide necessary support, assistance, and cooperation" and that "Article 17 allows Chinese intelligence agencies to take control of an organization's facilities, including communications equipment." *China Mobile USA Order*, 34 FCC Rcd at 3369, para. 17.

[73] *Pacific Networks/ComNet Order on Revocation and Termination*, 37 FCC Rcd at 4281, para. 70.

[74] *See China Telecom Americas Order on Revocation and Termination*, 36 FCC Rcd at 16003-04, para. 60 ("The combination of these laws—the 2017 Cybersecurity Law, the 2018 Cybersecurity Regulation, and the 2017 National Intelligence Law—raises substantial and serious national security risks."); *id.* at 16006, para. 63; *China Unicom Americas Order on Revocation*, 37 FCC Rcd at 1524, para. 67 (finding that "the combination of these laws—the 2017 Cybersecurity Law, the 2018 Cybersecurity Regulation, the 2017 National Intelligence Law, and the 2019 Cryptography Law—raises serious and significant national security risks"); *id.* at 1521-23, 1527-29, paras. 64-65, 69-71; *Pacific Networks/ComNet Order on Revocation and Termination*, 37 FCC Rcd at 4275, para. 63 ("We find that the combination of these laws—the 2017 Cybersecurity Law, its implementing regulation (2018 Cybersecurity Regulation), 2017 National Intelligence Law, and the 2019 Cryptography Law—raises substantial and serious national security and law enforcement risks."); *China Mobile USA Order*, 34 FCC Rcd at 3369, n.56 ("Other Chinese laws obligate citizens and organizations to cooperate with intelligence activities.").

these laws "'provide little, if any, detail about the available legal procedures or judicial oversight to challenge any Chinese government requests.'"[75] Digitalsystem has provided no persuasive argument to refute the significant concerns raised by the record that the government of China could require its majority owner—a citizen of China—and, consequently, Digitalsystem, to take certain actions in furtherance of the government of China's national intelligence goals through the requirements of the laws of China. The record demonstrates that Digitalsystem {[

]}[77] Based on the evidence in the record, we find that Digitalsystem, through its control and majority ownership by a citizen of China, is highly likely to be forced to comply with the government of China's requests without sufficient legal procedures subject to independent judicial oversight.[78]

13. Digitalsystem also failed to persuasively explain how these national security and law enforcement concerns associated with the government of China's jurisdiction can be ameliorated if Digitalsystem {[

]}[79]

Digitalsystem does not dispute the Committee's statements. Instead, Digitalsystem claims that it commits that "[n]o remote access to Digitalsystem's U.S. network management systems or lawful-intercept systems will be permitted from mainland China."[80] However, Digitalsystem has provided no evidence or persuasive argument to dispel the concerns raised by the record that it is highly likely to be forced to comply with the government of China's requests without sufficient legal procedures subject to independent judicial oversight.[81]

---

[75] *China Telecom Americas Order on Revocation and Termination*, 36 FCC Rcd at 16006, para. 62 (citing Executive Branch Recommendation to the Federal Communications Commission to Revoke and Terminate [CTA's] International Section 214 Common Carrier Authorizations, File Nos. ITC-214-20010613-00346, ITC-21420020716-00371, ITC-T/C-20070725-00285, at 40 (filed Apr. 9, 2020)); *see China Unicom Americas Order on Revocation*, 37 FCC Rcd at 1528-29, para. 71; *Pacific Networks/ComNet Order on Revocation and Termination*, 37 FCC Rcd at 4282-83, para. 71. The Committee explains that "[c]ourts have repeatedly acknowledged the national-security risks posed by the PRC legal regime and upheld the FCC and other U.S. Government national-security actions based on these risks, including with respect to Hong Kong locations and entities." Committee Recommendation at 13 & n.61 (citing *China Unicom (Ams.) Operations Ltd. v. FCC*, 124 F.4th at 1152; *China Telecom (Ams.) Corp.*, 57 F.4th at 263–65; *Pac. Networks Corp. v. FCC*, 77 F.4th at 1164; *TikTok Inc. & ByteDance Ltd. v. Garland*, 122 F.4th 930, 954 (D.C. Cir. 2024), *TikTok v. Garland*, 604 U.S. 56 (2025)).

[76] Committee Recommendation at 5 ({[ ]}).

[77] Committee Recommendation at 29; *id.* at 29-30 ({[

]}).

[78] Indeed, Digitalsystem acknowledges that it may be subject to "[a]ny request from a foreign government (including Hong Kong) for access to U.S. customer data or lawful-process information," and fails to explain how it would mitigate the risks at the time of any such request except to claim that it would notify the Committee "within 15 days." Digitalsystem Opposition at 4.

[79] Committee Recommendation at 18.

[80] Digitalsystem Opposition at 2.

[81] *See China Telecom Americas Order on Revocation and Termination*, 36 FCC Rcd at 15967, para. 2; *China Unicom Americas Order on Revocation*, 37 FCC Rcd at 1481, para. 2; *Pacific Networks/ComNet Order on Revocation and Termination*, 37 FCC Rcd at 4221, para. 2.

14. While Digitalsystem suggests that "[c]itizenship alone has never been a per se disqualifying factor for Section 214 authority,"[82] it is nonetheless certainly germane to the Commission's evaluation of whether grant is in the public interest, as reflected in the Commission's longstanding consideration of the citizenship of an applicant and its reportable interest holders.[83] Moreover, Digitalsystem's suggestion that "[c]itizenship alone has never been a per se disqualifying factor for Section 214 authority"[84] is beside the point, because the Commission does not treat it as a per se disqualifying factor today. Thus, when the Commission has in the past denied an application for international section 214 authority[85] and revoked the section 214 authority of certain entities, in assessing the entire record, it took into account the citizenship of the applicant's interest holders or that of the authorization holder as well as other national security and law enforcement concerns that had been raised, including that the applicant or the authorization holder is ultimately owned and controlled by the government of China.[86] In the *China Mobile USA Order*, *China Telecom Americas Order on Revocation and Termination*, *China Unicom Americas Order on Revocation*, and *Pacific Networks and ComNet Order on Revocation and Termination*, the Commission found that these entities are subject to exploitation, influence, and control by the Chinese government, and that mitigation would not address the national security and law enforcement concerns.[87] The circumstances here do not persuade us to the contrary, particularly given the concerns raised by the Committee regarding the applicant's susceptibility to the government of China's jurisdiction and control—including as well through its majority owner's {[ ]}[88] and its planned operations {[ ]}[89]—and the evidence in the record regarding the applicant's lack of trustworthiness,[90] as discussed herein.

15. In addition, the Commission has undertaken further actions to identify and mitigate foreign adversary threats to our nation's communications infrastructure based on the citizenship of individuals or entities—including where it concerns ownership, control, jurisdiction, or direction by foreign adversaries—such as those originating from the government of China.[91] In several proceedings,

[82] Digitalsystem Opposition at 2.

[83] *See supra* section II. Under section 63.18(b) of the rules, an applicant seeking international section 214 authority must identify "[t]he Government, State, or Territory under the laws of which each corporate or partnership applicant is organized." 47 CFR § 63.18(b). Under section 63.18(h) of the rules, an applicant must provide "[t]he name, address, citizenship, and principal businesses of any individual or entity that directly or indirectly owns ten percent or more of the equity interests and/or voting interests, or a controlling interest, of the applicant, and the percentage of equity and/or voting interest owned by each of those entities (to the nearest one percent)." 47 CFR § 63.18(h).

[84] Digitalsystem Opposition at 2.

[85] *China Mobile USA Order*, 34 FCC Rcd at 3361-62, para. 1.

[86] *China Telecom Americas Order on Revocation and Termination*, 36 FCC Rcd at 15966-67, para. 1; *Unicom Americas Order on Revocation*, 37 FCC Rcd at 1480-81, para. 1; *Pacific Networks and ComNet Order on Revocation and Termination*, 37 FCC Rcd at 4220-21, para. 1.

[87] *China Telecom Americas Order on Revocation and Termination*, 36 FCC Rcd at 15967, para. 2; *China Unicom Americas Order on Revocation*, 37 FCC Rcd at 1481, para. 2; *Pacific Networks and ComNet Order on Revocation and Termination*, 37 FCC Rcd at 4221-22, para. 2; *China Mobile USA Order*, 34 FCC Rcd at 3365-66, para. 8.

[88] *See supra* para. 10; *see infra* para. 31.

[89] *See infra* section III.B.3 and III.B.4.

[90] *See infra* section III.B.5.

[91] *See, e.g.*, *China Mobile USA Order*; *China Telecom Americas Order on Revocation and Termination*; *China Unicom Americas Order on Revocation*; *Pacific Networks/ComNet Order on Revocation and Termination*; *Promoting the Integrity and Security of Telecommunications Certification Bodies, Measurement Facilities, and the Equipment Authorization Program*, ET Docket No. 24-136, Report and Order and Further Notice of Proposed Rulemaking, 40 FCC Rcd 3616, 3617-19, paras. 2-3 (2025); *Review of Submarine Cable Landing License Rules and Procedures to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks*, OI (continued….)

the Commission used the Department of Commerce's definition of "foreign adversary" that was developed to implement Executive Order 13783,[92] and relied on the determinations of the Secretary of Commerce that currently identify six foreign adversaries including "The People's Republic of China, including the Hong Kong Special Administrative Region and the Macau Special Administrative Region (China)."[93] In several proceedings, the Commission has also adopted, with limited modifications, the Department of Commerce's definition in 15 CFR § 791.2, of an individual or entity "owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary."[94]

16. Consistent with the Committee's recommendation and the Commission's identification of foreign adversary threats in analogous contexts,[95] we find that the record demonstrates that both Digitalsystem and its majority owner, Hui Xie, are "owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary."[96] Hui Xie is a citizen of China and thus "[an] individual, wherever located, who is a citizen of a foreign adversary or a country controlled by a foreign adversary," as set out

Docket No. 24-523, MD Docket No. 24-524, Report and Order and Further Notice of Proposed Rulemaking, 40 FCC Rcd 6481 (2025) (*2025 Submarine Cable First Report and Order and FNPRM)*; corrected by Erratum, https://docs.fcc.gov/public/attachments/DOC-414544A1.pdf (OIA and OMD Sept. 16, 2025); corrected by Second Erratum, https://docs.fcc.gov/public/attachments/DOC-415107A1.pdf (OIA and OMD Oct. 24, 2025).

[92] *See* 15 CFR § 791.2 (defining "foreign adversary" as "any foreign government or foreign non-government person determined by the Secretary to have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons"); 15 CFR § 791.4 (identifying determination of foreign adversaries); Department of Commerce, Securing the Information and Communications Technology and Services Supply Chain, Interim Final Rule, 86 Fed. Reg. 4909-01 (Jan. 19, 2021); Department of Commerce, Redesignation of Regulations for Securing the Information and Communications Technology and Services Supply Chain, 89 Fed. Reg. 58263, 58264-65 (July 18, 2024); Department of Commerce, Securing the Information and Communications Technology and Services Supply Chain, 89 Fed. Reg. 96872 (Dec. 6, 2024); Executive Order 13873 of May 15, 2019, Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 22689 (May 17, 2019) (Executive Order 13873); *see Equipment Authorization Report and Order and FNPRM*, 40 FCC Rcd at 3639-40, paras. 44-48; *Protecting our Communications Networks by Promoting Transparency Regarding Foreign Adversary Control*, GN Docket No. 25-166, Report and Order, FCC 26-2, 2026 WL 297882, at *5-6, paras. 14-16 (2026) (*Foreign Adversary Control Report and Order*); *2025 Submarine Cable Report and Order*, 40 FCC Rcd at 6491-92, paras. 20-21; 47 CFR §§ 1.70001(e) (defining "Foreign adversary"), 8.217(d), 8.220(c)(7).

[93] 15 CFR § 791.4; *see Equipment Authorization Report and Order and FNPRM*, 40 FCC Rcd at 3639-40, paras. 44-48; *2025 Submarine Cable Report and Order*, 40 FCC Rcd at 6491-93, paras. 21-23; *Foreign Adversary Control Report and Order*, at *9-10, para. 22.

[94] *2025 Submarine Cable Report and Order*, 40 FCC Rcd at 6492-97, para. 23-29; *Foreign Adversary Control Report and Order*, at *6, para. 15; 47 CFR § 1.70001(g) (defining "Owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary").

[95] For example, in the context of submarine cables, the Commission adopted a presumption that an applicant that is "owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary" is not qualified to hold a cable landing license unless the applicant overcomes the adverse presumption. *2025 Submarine Cable Report and Order*, 40 FCC Rcd at 6497-6501, paras. 30-35; 47 CFR § 1.70004(a); *see also* Digitalsystem Opposition at 2 ("Citizenship alone has never been a per se disqualifying factor for Section 214 authority."). In the *Foreign Adversary Control Report and Order*, the Commission adopted rules requiring all Regulatees holding Covered Authorizations listed in Schedule A or that have an application for a Covered Authorization listed in Schedule A pending before the Commission to submit an attestation to the Commission that it is or is not owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary. *Foreign Adversary Control Report and Order*, * 27, 44, para. 61, Appx. A (§ 1.80002) (identifying international section 214 authorizations as "Schedule A Covered Authorizations").

[96] 47 CFR § 1.70001(g).

in section 1.70004(g)(2).[97] Digitalsystem is "owned or controlled by a foreign adversary," as set out in section 1.70004(g)(4), through Hui Xie, a citizen of China, "possess[ing] the power, direct or indirect, whether or not exercised, through the ownership of a majority . . . of the total outstanding voting interest and/or equity interest, or through a controlling interest, in [Digitalsystem] . . . to determine, direct, or decide important matters affecting [Digitalsystem]."[98] This analysis supports our fundamental concerns in this proceeding—namely, concerns over Digitalsystem's control, through Hui Xie's control and majority ownership of Digitalsystem, by a foreign adversary raising substantial and unacceptable national security and law enforcement risks—and our determination based on the Committee's Recommendation and the totality of these circumstances, collectively, that mitigation would not address those concerns.

2. Digitalsystem's Partnership with a Hong Kong Affiliate and Other Entities Raise National Security and Law Enforcement Risks

17. Based on the totality of the evidence in the record, we find that Digitalsystem's partnerships with a Hong Kong affiliate and {[ ]} raise significant national security and law enforcement concerns.[99] The Committee explains that Digitalsystem's "plans for its Section 214 authorization—which include services {[ ]}, partnership {[ ]} with {[ ]}, and relationships and potential relationships with {[ ]} service providers—exacerbate [the] risks."[100] The Committee states that if Digitalsystem is granted an international section 214 authorization, there is a significant risk that its international telecommunications services "could be exploited by PRC and Hong Kong-based threat actors to the detriment of U.S. interests, including the confidentiality and security of U.S. communications traffic and sensitive U.S. records."[101]

18. Specifically, the Committee states that "Digitalsystem's plans to provide services to and from Hong Kong, {[ ]} present[] national security concerns given how mainland China has steadily increased its control of Hong Kong, to the extent that Hong Kong today is 'no longer sufficiently autonomous to justify differential treatment' in relation to China."[102] Further, the Committee states that Digitalsystem {[

[97] 47 CFR § 1.70001(g)(2) ("The term 'owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary' as used in this subpart applies to . . . [a]ny individual, wherever located, who is a citizen of a foreign adversary or a country controlled by a foreign adversary, and is not a United States citizen or permanent resident of the United States."); 47 CFR § 1.70001(e).

[98] 47 CFR § 1.70001(g)(4) ("The term 'owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary' as used in this subpart applies to . . . [a]ny entity, including a corporation, partnership, association, or other organization, wherever organized or doing business, that is owned or controlled by a foreign adversary, to include circumstances in which any person identified in paragraphs (g)(1) through (3) of this section possesses the power, direct or indirect, whether or not exercised, through the ownership of a majority or a dominant minority (10% or greater) of the total outstanding voting interest and/or equity interest, or through a controlling interest, in an entity, board representation, proxy voting, a special share, contractual arrangements, formal or informal arrangements to act in concert, or other means, to determine, direct, or decide important matters affecting an entity.")

[99] Committee Recommendation at 18-28.

[100] Committee Recommendation at 38.

[101] Committee Recommendation at 38.

[102] Committee Recommendation at 14 (citing Exec. Order No. 13,936, 85 Fed. Reg. 43413, sec. 1 (July 14, 2020) (Executive Order 13936)); Executive Order 13936, sec. 1 ("It shall be the policy of the United States to suspend or eliminate different and preferential treatment for Hong Kong to the extent permitted by law and in the national security, foreign policy, and economic interest of the United States.").

]}[103] The Committee asserts that Digitalsystem's {[

]}[104] The Committee explains that the government of China has imposed its national security regime on Hong Kong,[105] including imposing the 2020 National Security Law that "enabled the PRC central government to assert greater control over the region."[106] In addition, the Committee states that "the law enforcement and security services of the two jurisdictions appear to be increasing their collaboration"[107] and, as of the 2020 National Security Law, "the PRC has increasingly exercised police and security power in Hong Kong."[108] The Committee raises concerns that Digitalsystem's Hong Kong affiliate, {[ ]} is directly subject to Hong Kong's jurisdiction and regulatory oversight."[109]

19. Digitalsystem argues generally that the Committee "relies heavily on generalized concerns about [China] and Hong Kong."[110] Digitalsystem, however, fails to offer sufficient rebuttal as to why those concerns do not apply to its situation. We agree with the Committee that Digitalsystem's partnership with a Hong Kong affiliate and other entities raise national security and law enforcement concerns. The Committee states that {[

]}[111] According to the Committee, {[

]}[113] As discussed above, Digitalsystem's majority owner is a citizen of China and therefore subject to the jurisdiction of the government of China and consequently the laws of China.[114] We agree with the Committee that Digitalsystem's partnership with its Hong Kong affiliate raises significant national security and law enforcement concerns given the Hong Kong affiliate is subject to the government of China's jurisdiction, including the government's national security regime,[115] and the record shows that {[

[103] Committee Recommendation at 34 ({[ ]}).

[104] Committee Recommendation at 34-35.

[105] *See* Committee Recommendation at 14-18.

[106] Committee Recommendation at 15. The Committee adds that, "should a conflict arise between Hong Kong's own data security law, the [Personal Data Privacy Ordinance] and the [2020 National Security Law], the [2020 National Security Law] could prevail." Committee Recommendation at 16.

[107] Committee Recommendation at 17.

[108] Committee Recommendation at 18.

[109] Committee Recommendation at 18.

[110] Digitalsystem Opposition at 1.

[111] Committee Recommendation at 6.

[112] Committee Recommendation at 6 ({[ ]}).

[113] Committee Recommendation at 6 ({[ ]}).

[114] *See supra* paras. 4, 10-16.

[115] Committee Recommendation at 18.

]}[116]

20. We reject Digitalsystem's claims that "the specific vulnerabilities the Committee identified concerning Hong Kong" would be eliminated by mitigation measures, including a commitment that "[s]haring of security tools, network engineering personnel, or security monitoring functions with the Hong Kong affiliate will cease within 60 days of any grant of authority."[117] Digitalsystem failed to persuasively explain how any measures would mitigate the risks associated with its plans to provide services to and from {[ ]}[118] an entity that is subject to the government of China's jurisdiction, and {[

]}[119] Digitalsystem presents no additional evidence or arguments that convince us that mitigation would be appropriate or adequate to address the national security and law enforcement risks identified by the Committee. Moreover, given the evidence in the record demonstrating Digitalsystem's lack of transparency, reliability, and consistent answers in its dealings with the Committee, as discussed below, we agree with the Committee that Digitalsystem "further eroded the trust required of a national-security mitigation partner,"[120] and is not likely to cooperate and be fully transparent with the Committee in such a way that would allow a mitigation agreement to be effective.[121]

21. The Committee also contends that Digitalsystem's planned and potential partnerships with {[ ]} entities—including {[ ]}—raise significant national security and law enforcement concerns.[122] The Committee argues that such entities "are subject to the jurisdiction, direction, and control of the PRC and Hong Kong governments, especially given these jurisdictions' ever-expanding national security laws" and "have significant intent and capability to harm U.S. national security and law enforcement interests through U.S. telecommunications companies."[123] As discussed below, the Committee explains there are "significant concerns with these relationships and Digitalsystem's ability to adequately mitigate risk stemming from these potential partnerships."[124]

22. The Committee states that Digitalsystem relies on {[

]}[125] The Committee identifies {[

]}[127] The Committee states that {[

[116] *See* Committee Recommendation at 6.

[117] Digitalsystem Opposition at 2-4.

[118] Committee Recommendation at 14.

[119] Committee Recommendation at 34.

[120] Committee Recommendation at 2.

[121] *See infra* section III.B.5.

[122] Committee Recommendation at 18-28.

[123] Committee Recommendation at 28.

[124] Committee Recommendation at 28.

[125] Committee Recommendation at 20.

[126] Committee Recommendation at 21 ({[

]}).

[127] Committee Recommendation at 21 {([

(continued….)

]}[128] According to the Committee, "Digitalsystem stated that, after it receives its international Section 214 authorization, {[
]}[129]
The Committee raises concerns that {[
]}[130] The Committee further states that, {[
]}[131]

23. In addition, the Committee asserts that Digitalsystem's current and future potential relationship with {[ ]} presents significant national security concerns.[132] The Committee notes that {[
]}[133] The Committee explains that Digitalsystem relies on {[
]}[134]
Further, the Committee states that Digitalsystem's response to the Committee's inquiries about its current and future plans regarding {[
]}[135] According to the Committee,
{[
]}[136]

24. The Committee also asserts that Digitalsystem's current or potential partnership with

]}).

[128] Committee Recommendation at 21. In addition to {[ ]} the Committee states that {[ ]} *Id.* at 20.

[129] Committee Recommendation at 20 ({[ ]}).

[130] Committee Recommendation at 20.

[131] Committee Recommendation at 21-22.

[132] Committee Recommendation at 22-24.

[133] Committee Recommendation at 22.

[134] Committee Recommendation at 22-23 (explaining, {[
]}).

[135] Committee Recommendation at 23 ({[
]}).

[136] Committee Recommendation at 24. In addition, the Committee states that ({[
]}).

{[ ]} presents significant national security and law enforcement concerns.[137] The Committee states that Digitalsystem provided conflicting responses regarding its partnership with {[ ]} as Digitalsystem initially represented that {[

]}[138] The Committee notes, however, that Digitalsystem's website identified{[ ]} as a "Partner," even though Digitalsystem stated in response to the Committee's subsequent inquiry that {[
]}[139] According to the Committee, Digitalsystem stated in response to the Committee's subsequent inquiry that {[

]}[140] The Committee raises a concern that {[
]}[141]

25. The Committee also identifies significant concerns regarding Digitalsystem's current or potential partnership with {[ ]} particularly in light of Digitalsystem's conflicting responses to the Committee.[142] As discussed above, despite Digitalsystem's initial representations to the contrary to the Committee,[143] Digitalsystem's website identified {[ ]} as a "Partner."[144] According to the Committee, Digitalsystem stated in response to the Committee's subsequent inquiry that {[

]}[145] The Committee notes, however, that Digitalsystem thereafter updated its website to remove the phrase "Partners," and instead identified the relevant companies under a banner reading "Clients who trust us."[146] The Committee states that "[t]his website description now implies that the listed companies are customers of Digitalsystem, {[
]}[147] The

[137] Committee Recommendation at 26-27.

[138] Committee Recommendation at 26 ({[ ]}); *see id.* at 8, n.37 (addressing Executive Order 13873).

[139] Committee Recommendation at 26 ({[ ]}).

[140] Committee Recommendation at 27.

[141] Committee Recommendation at 27. The Committee further notes that {[

]} Committee Recommendation at 27 ({[

]}).

[142] Committee Recommendation at 26-28. The Committee also notes that {[

]} Committee Recommendation at 28 ({[

]}).

[143] *See supra* para. 23.

[144] Committee Recommendation at 26.

[145] Committee Recommendation at 26-27.

[146] Committee Recommendation at 28.

[147] Committee Recommendation at 28.

Committee also states that Digitalsystem provided inconsistent responses regarding future business with {[ ]}[148]

26. Digitalsystem argues that it is "a small reseller and facilities-based applicant, not a strategic partner of these carriers."[149] Digitalsystem, however, does not dispute the Committee's arguments regarding the national security and law enforcement risks associated with its current or potential partnerships with these {[ ]} entities. Instead, Digitalsystem claims that "[e]very substantive vulnerability identified in the confidential Recommendation is now directly addressed by a specific, verifiable commitment,"[150] including three commitments regarding "[p]artnerships with PCCW, China Unicom, and China Mobile."[151] Specifically, Digitalsystem states that "[i]ts current testing connections to PCCW and China Unicom are not commercial telecommunications services to end users."[152] In addition, Digitalsystem states that "[n]o U.S. customer communications content is routed through China Unicom or China Mobile."[153] Finally, Digitalsystem states that, "[t]o eliminate any uncertainty, Digitalsystem commits that it will not enter into any new interconnection or partnership agreement with China Unicom, China Mobile, or any PRC state-owned carrier without prior written notice to the Committee, and will comply with any future FCC Covered List determinations."[154] This approach does not address issues regarding concerns in the record regarding Digitalsystem's current business relationships and its overall trustworthiness, however.

27. In fact, Digitalsystem does not deny any partnership and the associated national security and law enforcement risks. Nor does Digitalsystem make any commitment to *not* enter into these partnerships, but instead states that it will not enter into "any new interconnection or partnership agreement" with these entities "*without prior written notice to the Committee*,"[155] while wholly ignoring the concerns raised by the Committee regarding partnerships with {[ ]} and failing to provide any additional commitment if the Committee were to reiterate the objections that it has already raised in the record. Digitalsystem also fails to persuasively explain how the significant risks surrounding any current or future partnerships, including {[ ]} by entities that "have significant intent and capability to harm U.S. national security and law enforcement interests,"[156] could be ameliorated. Moreover, Digitalsystem wholly ignores the specific risks identified by the Committee regarding its current or potential partnership with {[ ]} Further, the record demonstrates that Digitalsystem {[ ]}[157] and represented to the Committee that, {[ ]}[158] Digitalsystem does not dispute the Committee's statements or

[148] Committee Recommendation at 28 ({[ ]}).

[149] Digitalsystem Opposition at 2.

[150] Digitalsystem Opposition at 5.

[151] Digitalsystem Opposition at 2.

[152] Digitalsystem Opposition at 2.

[153] Digitalsystem Opposition at 2.

[154] Digitalsystem Opposition at 3.

[155] Digitalsystem Opposition at 3 (emphasis added).

[156] Committee Recommendation at 28; *see supra* paras. 21-25.

[157] Committee Recommendation at 20.

[158] Committee Recommendation at 20 ({[ ]}).

explain how mitigation measures would fully address the risks. We find that the record reflecting Digitalsystem's relationships with {[ ]} entities and Digitalsystem's responses to the Committee's inquiries with respect thereto, combined with the government of China's jurisdiction and control over Digitalsystem,[159] raise serious concerns as to whether Digitalsystem can be trusted to cooperate with the Committee's mitigation monitoring in good faith and with transparency, and to comply with mitigation terms.

3. Digitalsystem's Planned Operations Concerning U.S. Records and Cybersecurity Present National Security and Law Enforcement Risks

28. In addition to Digitalsystem's planned partnerships, we also find that Digitalsystem's planned operations for storage of and access to U.S. records and cybersecurity practices raise significant national security and law enforcement concerns.

29. *Storage of and Access to U.S. Records*. The Committee asserts there are significant vulnerabilities raised by Digitalsystem's storage of U.S. records and data in {[ ]}[160] The Committee explains that, if granted authority to provide both facilities-based and resold services, Digitalsystem "would directly handle communications and access U.S. customer records and communications related data, including PII, Call Detail Records ('CDRs'), bill records, and more."[161] The Committee states that Digitalsystem {[

]}[162] The Committee raises concerns that, {[

]}[163] The Committee states that {[

]}[164]

30. Additionally, the Committee identifies significant concerns raised by {[

]}[165] The Committee states that, "[d]espite repeated questioning by the Committee, Digitalsystem never provided the Committee a full accounting of the vendors, locations of access, or number of foreign individuals that are expected to have access to Digitalsystem's U.S. records and systems.[166] The Committee explains that, {[

[159] *See supra* section III.B.1.

[160] Committee Recommendation at 33-34.

[161] Committee Recommendation at 33.

[162] Committee Recommendation at 33.

[163] Committee Recommendation at 34 ({[ ]}).

[164] Committee Recommendation at 34.

[165] *Id.* at 30-32.

[166] *Id.* at 31. According to the Committee, "Digitalsystem initially stated {[

]} However, Digitalsystem later revealed that {[

]} *Id.* at 30-31.

]}[167] According to the Committee, {[

]}[168] Moreover, according to the Committee, {[

]}[169] The Committee explains that {[

]}[170]

31. Further, the Committee raises concerns that Digitalsystem "provided misleading responses regarding the extent of its owners' access to company records and systems,"[171] and addresses {[ ]} The Committee explains that, {[

]}[172] The Committee also explains that {[

]}[173] Significantly, the Committee states that {[

]}[174]

32. Digitalsystem again argues generally that the Committee "relies heavily on generalized

[167] *Id.* at 31.

[168] *Id.* at 31 ({[

]}).

[169] *Id.* at 32 ({[ ]}). Further, the Committee explains that {[

]} *Id.* at 31 ({[ ]}).

[170] *Id.* at 32.

[171] *Id.* at 29.

[172] *Id.* at 30. According to the Committee, "Digitalsystem's responses originally described {[

]}). *Id.* at 29. The Committee explains, {[

]}. *Id.*

[173] *Id.* at 30 ({[ ]}).

[174] *Id.* at 30; *id.* at 32 ({[

]}).

concerns about [China] and Hong Kong."[175] Digitalsystem, however, fails to offer sufficient rebuttal as to why those concerns do not apply to its situation. Instead, Digitalsystem claims that "the specific vulnerabilities the Committee identified concerning Hong Kong" would be eliminated by mitigation measures, including a commitment that "[n]o U.S. customer records, call detail records (CDRs), or communications content will be stored in Hong Kong or mainland China, including backups."[176] Digitalsystem also argues that "it never intentionally misled the Committee" regarding "[t]he extent of owners' access to systems" and "[f]oreign individuals with access to U.S. records."[177] Digitalsystem asserts that it "ultimately provided the requested information, including the identity of service providers, access locations, and security practices."[178]

33. Based on our consideration of the totality of the record evidence, we reject Digitalsystem's argument that mitigation would be appropriate or adequate to address these national security and law enforcement risks identified by the Committee. As an initial matter, the record shows that Digitalsystem {[ ]}[179] which Digitalsystem does not dispute. In addition, based on the record, Digitalsystem plans to provide services to and from {[ ]}[180] an entity that "is directly subject to Hong Kong's jurisdiction and regulatory oversight,"[181] and {[ ]}[182] which Digitalsystem neither disputes nor addresses with specificity how it would mitigate risks associated with storage of and access to U.S. records in {[ ]} Moreover, the record shows that {[ ]}[183] which Digitalsystem also does not dispute or explain how it would mitigate the identified risks.

34. We find that the storage of and access to {[ ]} raise serious national security and law enforcement concerns that cannot be mitigated, given {[ ]}[184] As discussed above, Digitalsystem, through its control and majority ownership by a citizen of China, is subject to the government of China's jurisdiction and control.[185] Digitalsystem has failed to persuasively explain how mitigation would fully address the national security and law enforcement concerns presented by the requirements of the laws of China that would compel Digitalsystem and its majority owner, a citizen of China, to comply with requests from the government of China, including where it concerns storage of and access to U.S. records.[186] Moreover, notwithstanding

[175] Digitalsystem Opposition at 1.

[176] Digitalsystem Opposition at 2.

[177] *Id.* at 3.

[178] *Id.* at 3.

[179] Committee Recommendation at 33-34.

[180] Committee Recommendation at 14.

[181] Committee Recommendation at 18.

[182] Committee Recommendation at 34-35; *see supra* para. 18.

[183] *Id.* at 31-32.

[184] Committee Recommendation at 34.

[185] *See supra* section III.B.1.

[186] *See supra* section III.B.1. As discussed above, the Committee states that the government of China, through laws such as the 2017 National Intelligence Law, could compel Hui Xie "to cooperate, assist, and support Chinese (continued….)

any commitment regarding the storage of U.S. records in Hong Kong and China, Digitalsystem has also failed to persuasively explain how the significant risks surrounding any current or future relationships with {[ ]} entities, including {[ ]} by such entities,[187] could be ameliorated.[188] Finally, we are unpersuaded by Digitalsystem's claim that it rectified its incomplete and inconsistent responses to the Committee, given the evidence in the record demonstrating Digitalsystem's lack of transparency and reliability in its dealings with the Committee. Digitalsystem fails to adequately refute, for example, the Committee's argument that "Digitalsystem never provided the Committee a full accounting of the vendors, locations of access, or number of foreign individuals that are expected to have access to Digitalsystem's U.S. records and systems," which consequently "impeded the Committee's ability to fully assess the risks associated with such access and consider appropriate mitigation measures to address those risks."[189] We agree with the Committee that Digitalsystem is not likely to cooperate and be fully transparent with the Committee in such a way that would allow a mitigation agreement to be effective.[190]

35. *Cybersecurity and Lawful U.S. Processes.* The Committee asserts that {[ ]}[191] The Committee further explains that Digitalsystem's {[ ]}[192] In addition, the Committee raises a concern that {[ ]}[193] The Committee explains that {[ ]}[194] The Committee states that, {[

intelligence efforts, even though he resides in the United States." Committee Recommendation at 18. Among other things, the Committee explains that the 2020 Data Security Law "expands the PRC government's access to, and control of, companies and data within the PRC and subjects cross-border data flows to additional regulatory requirements and prohibitions." Committee Recommendation at 11-12 (citing U.S. Dep't of Homeland Sec., Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China at 7–8 (Dec. 22, 2020), https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf). Moreover, the Committee explains "the Committee's national security concerns regarding telecommunications connectivity with Hong Kong, as the [2020 National Security Law] erodes Hong Kong's autonomy and ability to operate independently of the PRC central government." Committee Recommendation at 16-17.

[187] *See supra* section III.B.2, para. 30.

[188] *See supra* section III.B.2.

[189] Committee Recommendation at 31.

[190] *See infra* section III.B.5.

[191] Committee Recommendation at 35.

[192] Committee Recommendation at 35.

[193] Committee Recommendation at 35.

[194] Committee Recommendation at 35-36.

]}[195]

36. Moreover, the Committee raises concerns about Digitalsystem's responses regarding its lawful U.S. processes and lawful intercept capabilities, given {[

]}[196] According to the Committee, "Digitalsystem initially stated that {[

]}[198] The Committee also explains that, {[

]}[199] The Committee states that {[

]}[200]

37. Digitalsystem does not dispute the Committee's assertion "that security roles described in Digitalsystem's policies are actually fulfilled by Mr. Xie and Ms. Zhou and that no independent CISO exists,"[201] and acknowledges "[t]his criticism is factually accurate and is accepted by Digitalsystem as a basis for improvement."[202] However, Digitalsystem states that "[e]very substantive vulnerability identified in the confidential Recommendation is now directly addressed by a specific, verifiable commitment,"[203] including two commitments related to "Security Governance and Absence of an Independent CISO."[204] Specifically, Digitalsystem states that it commits to "[a]ppointing a qualified, independent [CISO] who is not Mr. Xie or Ms. Zhou, with authority over U.S. network security, access controls, and compliance with FCC and law enforcement requirements."[205] Digitalsystem also states that "[t]he independent CISO's identity and qualifications will be submitted to the FCC and Committee within 60 days of any grant."[206]

38. Digitalsystem, however, claims that "[t]he core alleged inconsistency regarding CALEA is easily explained"—according to Digitalsystem, it "does not yet have a Section 214 authorization, therefore it has not deployed production-level lawful-intercept equipment," but "[u]pon grant, it will fully comply with CALEA and law enforcement process."[207] Digitalsystem argues that "[t]here is no

[195] Committee Recommendation at 36.

[196] Committee Recommendation at 33.

[197] Committee Recommendation at 32.

[198] Committee Recommendation at 32-33.

[199] Committee Recommendation at 33. According to the Committee, {[ ]} Committee Recommendation at 33 ({[ ]}).

[200] Committee Recommendation at 33.

[201] Digitalsystem Opposition at 3.

[202] Digitalsystem Opposition at 3.

[203] Digitalsystem Opposition at 5.

[204] Digitalsystem Opposition at 3-4.

[205] Digitalsystem Opposition at 3-4.

[206] Digitalsystem Opposition at 4.

[207] Digitalsystem Opposition at 3.

inconsistency when read in context."[208] Further, Digitalsystem states that "[e]very substantive vulnerability identified in the confidential Recommendation is now directly addressed by a specific, verifiable commitment,"[209] including commitments, upon grant, to "[d]eploy CALEA-compliant solutions," "[d]esignate a U.S.-based law enforcement point of contact," and "[p]rovide the Committee with a written lawful-intercept implementation plan within 90 days."[210]

39. We are unpersuaded by Digitalsystem's argument that it has addressed "[e]very substantive vulnerability" required to mitigate the identified cybersecurity risks.[211] As an initial mater, Digitalsystem states generally that it commits to "[a]ppointing a qualified, independent [CISO],"[212] but does not address with particularity what qualifications it would consider for this role.[213] Digitalsystem presents no additional evidence or arguments that convince us that mitigation would be adequate here, especially given {[

]}[215] We agree with the Committee that Digitalsystem's {[

]}[216] which Digitalsystem neither disputes nor persuasively explains can be mitigated.

40. Digitalsystem also does not dispute the Committee's assertions that {[

]}[218] Digitalsystem, however, wholly ignores the specific risks identified by the Committee regarding {[

]}[219] and only contends that it provided to the Committee "requested information, including . . . security practices."[220] Despite the Committee's emphasis on {[

]}[221] Digitalsystem has failed to persuasively explain whether or how it would {[

]}[222] Further, Digitalsystem did not {[

[208] Digitalsystem Opposition at 4.

[209] Digitalsystem Opposition at 5.

[210] Digitalsystem Opposition at 3-4.

[211] Digitalsystem Opposition at 3-5.

[212] Digitalsystem Opposition at 3.

[213] *See* Digitalsystem Opposition at 4 (stating that "[t]he independent CISO's identity and qualifications will be submitted to the FCC and the Committee within 60 days of any grant").

[214] *See supra* section III.B.2.

[215] Committee Recommendation at 36.

[216] Committee Recommendation at 36.

[217] Committee Recommendation at 35.

[218] Committee Recommendation at 35.

[219] Committee Recommendation at 35.

[220] Digitalsystem Opposition at 3.

[221] Committee Recommendation at 36.

[222] Committee Recommendation at 35.

[223] Committee Recommendation at 36.

]} Therefore, we reject Digitalsystem's suggestion that the cybersecurity risks identified in the record are fully mitigated here.[226]

41. We also reject Digitalsystem's contention that "[t]here is no inconsistency" in its representations to the Committee regarding its lawful U.S. process and lawful intercept capabilities.[227] The record is clear that Digitalsystem provided conflicting information to the Committee regarding its lawful U.S. process and lawful intercept capabilities.[228] We also agree with the Committee that the record demonstrates {[ ]}[229] In addition, Digitalsystem does not dispute that it provided conflicting information regarding {[ ]}[230] while it now states inconsistently that it commits to "[d]esignat[ing] a U.S.-based law enforcement point of contact."[231] Digitalsystem neither clarifies these discrepancies, including {[ ]}[232] nor addresses the Committee's assertion that {[ ]}[233] Given our findings herein that {[ ]} and the evidence in the record demonstrating Digitalsystem's lack of transparency and reliability in its dealings with the Committee, we find wholly unpersuasive Digitalsystem's suggestion that "[t]he alleged 'inconsistencies' have been corrected"[234] and that the risks identified in the record are fully mitigated here.[235]

4. Grant of the International Section 214 Authorization Would Produce Serious and Substantial National Security and Law Enforcement Risks

42. Based on the evidence in the record, we find that if Digitalsystem is granted an international section 214 authorization, there would be significant negative consequences for U.S. national security and law enforcement interests given the potential for the governments of China and

[224] Committee Recommendation at 35.

[225] *See* Committee Recommendation at 35.

[226] Digitalsystem Opposition at 3-5.

[227] Digitalsystem Opposition at 4.

[228] Based on the record, Digitalsystem initially represented to the Committee that {[ ]} Committee Recommendation at 32 (emphasis added). {[ ]} Committee Recommendation at 33.

[229] Committee Recommendation at 33.

[230] Committee Recommendation at 33.

[231] Digitalsystem Opposition at 4.

[232] *See* Committee Recommendation at 33 ({[ ]}).

[233] Committee Recommendation at 33.

[234] Digitalsystem Opposition at 5.

[235] Digitalsystem Opposition at 3-5.

Hong Kong and other threat actors to exploit the vulnerabilities associated with Digitalsystem.[236] First, the Committee argues that, "[i]f the vulnerabilities associated with Digitalsystem's business were exploited, threat actors could collect or exfiltrate communications content and sensitive records from U.S. customers and businesses."[237] Second, the Committee argues that, "[a]s Digitalsystem is planning to offer facilities-based, in addition to resold, services, a threat actor exploiting the vulnerabilities present with Digitalsystem's business could disrupt or impede the flow of communications."[238] Specifically, the Committee states that "[a] threat actor could target Digitalsystem's networks and equipment in the United States—{[ ]}—and access or prevent the equipment from working properly."[239] Third, the Committee asserts that "[a] threat actor seeking to exploit Digitalsystem could use Digitalsystem's equipment and networks to misroute U.S. communications and internet traffic to unintended foreign jurisdictions, including {[ ]}[240] The Committee states that if a party could gain control over Digitalsystem's management network—including, for example, "Digitalsystem itself, Digitalsystem's Hong Kong affiliate, a third-party with access to Digitalsystem's network, or a telecommunications provider with which Digitalsystem interconnects (such as {[ ]})"—such party "could direct traffic intended for the United States or other locations through Hong Kong or mainland China."[241] The Committee contends that this "would potentially expose U.S. communications and traffic to the security and intelligence services of these jurisdictions and, given the broadly defined 'national security' laws of these jurisdictions, and the limited options for legal [recourse] to protect sensitive data, would likely allow for collection of this data."[242]

43. Finally, the Committee argues that, given the evidence in the record, {[ ]}[243] The Committee explains there could be significant consequences for U.S. law enforcement and national security equities "[i]f these vulnerabilities were exploited by threat actors

[236] According to the Committee, "[w]hile the impact associated with {[ ]} the impact would increase as Digitalsystem gains an international Section 214 authorization and starts serving {[ ]} telecommunications customers. Committee Recommendation at 36. The Committee states that Digitalsystem {[ ]} Committee Recommendation at 36. The Committee explains that "this customer base would likely expand once Digitalsystem receives an international Section 214 authorization," whereupon "Digitalsystem intends to expand its telecommunications service offerings and customer base, focusing generally on {[ ]} Committee Recommendation at 36.

[237] Committee Recommendation at 37. The Committee states that such information could be used by "PRC and/or Hong Kong threat actors, to target particular individuals, such as dissidents in the United States, or particular businesses (for example, to gain access to trade secrets or other intellectual property)." Committee Recommendation at 37. According to the Committee, "[i]n the aggregate, the information could also enable bulk collection and analysis of information on U.S. persons." Committee Recommendation at 37.

[238] Committee Recommendation at 37.

[239] Committee Recommendation at 37. The Committee explains that, depending on the type and extent of Digitalsystem's future customer base, this situation could affect certain populations and industries. Committee Recommendation at 37.

[240] Committee Recommendation at 37.

[241] Committee Recommendation at 37.

[242] Committee Recommendation at 37.

[243] Committee Recommendation at 38.

including PRC intelligence services."[244]

44. Digitalsystem argues generally that the Committee "relies heavily on generalized concerns about [China] and Hong Kong."[245] Digitalsystem further claims that "the specific vulnerabilities the Committee identified concerning Hong Kong" would be eliminated by mitigation measures, including a commitment that "[a]ny request from a foreign government (including Hong Kong) for access to U.S. customer data or lawful-process information shall be reported to the Committee within 15 days,"[246] as well as other commitments that we discuss above.[247] Digitalsystem also claims that "[e]very substantive vulnerability identified in the confidential Recommendation is now directly addressed by a specific, verifiable commitment."[248]

45. Based on the totality of the evidence in the record, we reject Digitalsystem's argument that the national security and law enforcement concerns identified by the Committee, including Digitalsystem's vulnerability to China and Hong Kong threat actors, are "generalized concerns."[249] Consistent with Executive Order 13913,[250] the record demonstrates that the Committee specifically determined that "Digitalsystem's application presents risks to the national security and law enforcement interests of the United States,"[251] and assessed "[t]hese risks are posed in part by the government of [China], which presents significant threats within *the context of this application*."[252] We find that the record evidence, including the representations and responses provided by Digitalsystem, supports the Committee's identification of these specific national security and law enforcement risks associated with Digitalsystem, including its vulnerability to exploitation by the governments of China and Hong Kong

[244] Committee Recommendation at 38. The Committee asserts that "[e]xploitation of Digitalsystem's lawful U.S. process system could expose sensitive information about the targets of law enforcement or national security investigations and operational details about law enforcement and national security investigations themselves." Committee Recommendation at 38.

[245] Digitalsystem Opposition at 1.

[246] Digitalsystem Opposition at 4.

[247] *See supra* sections III.B.1-B.3.

[248] Digitalsystem Opposition at 5.

[249] Digitalsystem Opposition at 1.

[250] Under Executive Order 13913, the Committee shall "review applications . . . for risks to national security and law enforcement interests *posed by such applications*," and "respond to *any risks presented by applications* . . . by recommending to the FCC, as appropriate and consistent with the provisions of this order, that it dismiss an application, deny an application, condition the grant of an application upon compliance with mitigation measures . . . ." Executive Order 13913, 85 Fed. Reg. at 19643, sec. 3(a) (emphasis added); Committee Recommendation at 3 ("The Committee reviews applications referred by the FCC for risks to U.S. national security and law enforcement interests."). Pursuant to section 7(a), for each application reviewed by the Committee, the Director of National Intelligence produces "a written assessment of any threat to national security interests of the United States posted by granting the specific application." Executive Order 13913, 85 Fed. Reg. at 19646, sec. 7(a). The analysis required under section 7(a) is provided to the Committee. Executive Order 13913, 85 Fed. Reg. at 19646, sec. 7(b). Any recommendation made by the Committee with respect to an application, including a recommendation to deny the application, must be based on a written risk-based analysis. Executive Order 13913, 85 Fed. Reg. at 19647, sec. 9(c). The Committee must recommend that the Commission deny the application or that it only grant the license contingent on compliance with mitigation measures, "if [the Committee] determines that there is credible evidence that the application or license poses a risk to the national security or law enforcement interests of the United States." Executive Order 13913, 85 Fed. Reg. at 19647-48, sec. 9(d), 10(a). Here, the Committee recommends that "this particular application for international Section 214 authority should be denied because Digitalsystem's application presents risks to the national security and law enforcement interests of the United States that cannot be adequately mitigated." Committee Recommendation at 1.

[251] Committee Recommendation at 1.

[252] Committee Recommendation at 1 (emphasis added).

and other threat actors. The Committee explains, for example, that "Digitalsystem intends to use its Section 214 authorization to provide services to {[

]}[253] The Committee also explains that {[

]}[254] Digitalsystem fails to refute these significant concerns.

46. For these reasons, we also reject Digitalsystem's argument that "[e]very substantive vulnerability" identified by the Committee, including Digitalsystem's vulnerability to China and Hong Kong threat actors, has been "eliminated" or "addressed by a specific, verifiable commitment."[255] As previously stated by the Commission, fundamental to protecting the security of the United States is the ability to trust that a service provider will uphold the confidentiality and integrity of information on the traffic that it stores or transmits.[256] Based on the evidence in the record, Digitalsystem is subject to the jurisdiction and control of the government of China, which Digitalsystem fails to persuasively refute.[257] Significantly, Digitalsystem acknowledges it may be subject to "[a]ny request from a foreign government (including Hong Kong) for access to U.S. customer data or lawful-process information,"[258] and fails to explain how it would mitigate the risks at the time of any such request except to claim that it would notify the Committee "within 15 days."[259] Moreover, Digitalsystem's conduct and representations to the Committee demonstrate a lack of trustworthiness and reliability that erodes the baseline level of trust that the Commission and other U.S. government agencies require of telecommunications carriers given the critical nature of the provision of telecommunications service in the United States.[260] Given a mitigation agreement requires a baseline level of trust between the relevant parties to the agreement, and such trust is absent here, we find that Digitalsystem failed to provide any additional persuasive record support that would allow a mitigation agreement to be effective. We therefore agree with the Committee that there would be significant negative consequences for U.S. national security and law enforcement interests if Digitalsystem is granted an international section 214 authorization.

5. The National Security and Law Enforcement Risks Cannot be Mitigated

47. Based on the record, we find that mitigation would not address the significant national security and law enforcement concerns present in this case. We have a longstanding policy of according deference to the Executive Branch agencies' expertise in identifying risks to national security and law

[253] Committee Recommendation at 1.

[254] Committee Recommendation at 1.

[255] Digitalsystem Opposition at 5.

[256] *China Telecom Americas Order on Revocation and Termination*, 36 FCC Rcd at 16019, para. 81; *China Unicom Americas Order on Revocation*, 37 FCC Rcd at 1544, para. 93; *Pacific Networks and ComNet Order on Revocation and Termination*, 37 FCC Rcd at 4292-93, para. 82.

[257] *See supra* section III.B.1.

[258] Digitalsystem Opposition at 4.

[259] *Id.*

[260] Committee Recommendation at 2 ("Digitalsystem's representations during the Committee's review have further eroded the trust required of a national-security mitigation partner."); *see China Telecom Americas Order on Revocation and Termination*, 36 FCC Rcd at 16030-31, para. 100 ("[C]arriers sit at a privileged position and trust is paramount given the critical nature of the provision of telecommunications service in the United States."); *China Unicom Americas Order on Revocation*, 37 FCC Rcd at 1556, para. 111; *Pacific Networks and ComNet Order on Revocation and Termination*, 37 FCC Rcd at 4315, para. 115.

enforcement interests.[261] The Committee, which has expertise in matters of national security and law enforcement and in monitoring carriers' compliance with risk mitigation agreements, states that, "[g]iven {[ ]} Digitalsystem could not be a trusted party to an agreement with the Committee to potentially mitigate the specific risks posed by this application."[262] In addition, the Committee states that "Digitalsystem's representations during the Committee's review have further eroded the trust required of a national-security mitigation partner."[263] We agree with the Committee that the record evidence clearly demonstrates that the Commission and the Committee cannot trust or rely on Digitalsystem to adhere to mitigation measures, or to report any mitigation violations.

48. The Committee explains that "[c]omplete, coherent, and truthful responses are essential to the Committee's ability to assess and mitigate risks to U.S. national security and law enforcement interests associated with license applications, as well as the FCC's ability to enforce licensing conditions on a company should mitigation measures be imposed."[264] The Committee states that multiple federal courts have recognized, in the context of upholding the Commission's revocation and/or termination actions, that "[h]onesty and transparency with government agencies are important to assessing an 'authorization holder's ability to comply with the FCC's statutory authority and implementing rules,'" which is even more important "when the subject matter giving rise to the agency's concern about a company's trustworthiness involve that company's connections to a foreign power whose activities raise grave national security concerns."[265]

49. The Committee states that, throughout its review, "Digitalsystem provided conflicting responses, changed its responses, or did not provide complete information, raising doubts regarding its candor and ability to engage in a productive compliance relationship."[266] In particular, the Committee states that "[i]t appears . . . that Digitalsystem often provided an initial response that suggested a stronger security position than Digitalsystem was able to support upon follow-up questioning."[267] The Committee also raises concerns with Digitalsystem's conflicting or misleading answers regarding {[ ]};[269] the extent of access by Digitalsystem's owners, {[ ]}, to company records and systems;[270] "the number and location of foreign individuals with access

[261] *China Telecom Americas Order on Revocation and Termination*, 36 FCC Rcd at 16056, para. 139; *China Unicom Americas Order on Revocation*, 37 FCC Rcd at 1563, para. 124; *Pacific Networks and ComNet Order on Revocation and Termination*, 37 FCC Rcd at 4345, para. 152. Here, we defer to the Committee's expertise in identifying the risks that are reflected in the record and assessing whether any mitigation measures would resolve "a risk to the national security or law enforcement interests of the United States arising from the application." *See* Executive Order 13913, 85 FCC Rcd at 19648, sec. 10(a).

[262] Committee Recommendation at 2.

[263] Committee Recommendation at 2.

[264] Committee Recommendation at 24.

[265] Committee Recommendation at 24 (citing *China Unicom (Am.) Operations Ltd. v. FCC*, 124 F.4th at 1154; *China Telecom (Ams.) Corp. v. FCC*, 57 F.4th at 267–68; *Pac. Networks Corp. v. FCC*, 77 F.4th at 1165).

[266] Committee Recommendation at 24.

[267] Committee Recommendation at 24-25.

[268] Committee Recommendation at 25 (emphasis omitted).

[269] Committee Recommendation at 26-28.

[270] Committee Recommendation at 29-30.

to Digitalsystem's U.S. records, data, and equipment";[271] and "its lawful U.S. process and lawful intercept capabilities."[272]

50. Digitalsystem presents no additional persuasive evidence or arguments that convince us that mitigation would be appropriate or adequate to address the significant national security and law enforcement concerns. The Committee has not suggested that its concerns would be addressed by specific measures that Digitalsystem identified, further supporting our view that any mitigation measures offered in the Opposition are inadequate to address the concerns raised in this record. Indeed, Digitalsystem did not address with particularity or otherwise respond to the concerns identified by the Committee except to state that, "acknowledg[ing] that as a small company without prior experience in FCC national security reviews, some of its initial responses were insufficiently precise"[273] but that it "ultimately provided the requested information, including the identity of service providers, access locations, and security practices."[274] We find this argument wholly unpersuasive. That Digitalsystem claims it is a "small company" is not dispositive in our analysis and, importantly, should not hinder Digitalsystem's ability to produce fulsome and accurate information to U.S. government agencies and cooperate with the Committee. For example, Digitalsystem states there is no inconsistency in its responses to the Committee's inquiries, such as its descriptions of its CALEA capabilities.[275] We agree with the Committee that Digitalsystem fails to understand the fundamental concern with how Digitalsystem {[ ]}[276] and as a consequence, this raises serious doubts regarding Digitalsystem's truthfulness and transparency regarding a critical technical requirement that is essential for law enforcement agencies and Digitalsystem's ability to comply with CALEA if granted an international section 214 authorization. As the Commission has previously stated, "'because the underlying foundation of trust that is needed for a mitigation agreement of this type to adequately address national security and law enforcement concerns is not present, the opportunity for effective mitigation . . . is illusory at best in the current national security environment.'"[277]

51. Ultimately, Digitalsystem disagrees with the fundamental concerns in this proceeding that Digitalsystem is not a trusted party, and instead contends that the Committee's assessment that the risks are unmitigable "is not supported by the record" and that "[e]very substantive vulnerability identified in the confidential Recommendation is now directly addressed by a specific, verifiable commitment."[278] Digitalsystem further contends that denial of its application would be "disproportionate" and that "[t]he appropriate outcome is a conditional grant with mitigation measures" or the Commission should "remand to the Committee for negotiation of a formal mitigation agreement."[279] We disagree. As discussed above, the evidence in the record overwhelmingly shows that Digitalsystem provided

[271] Committee Recommendation at 30-32.

[272] Committee Recommendation at 32-33. As discussed above, the Committee explains that "Digitalsystem initially stated that{[ ]} Committee Recommendation at 32; *see supra* section III.B.4.

[273] Digitalsystem Opposition at 3.

[274] Digitalsystem Opposition at 3.

[275] Digitalsystem Opposition at 3-4.

[276] Committee Recommendation at 33.

[277] *See China Unicom Americas Order on Revocation*, 37 FCC Rcd at 1563, para. 124.

[278] Digitalsystem Opposition at 4s (stating, for example, that it commits to conditions such as appointing an "[i]ndependent CISO," "[n]o Hong Kong/China data storage," "[n]o remote access from mainland China," "[a]ffiliate separation," "[u]nconditional government inspection," and reporting "[a]ny request from a foreign government (including Hong Kong) for access to U.S. customer data or lawful-process information" to the Committee within 15days).

[279] *Id*.

inconsistent and changed responses throughout the Committee's review, which raises serious doubts as to Digitalsystem's trustworthiness and reliability. Moreover, Digitalsystem fails to recognize the significant and substantial national security and law enforcement risks associated with the government of China's jurisdiction and control over Digitalsystem and its vulnerability to exploitation by China and Hong Kong threat actors. Based on the record, we find that Digitalsystem cannot be trusted by the Committee and the Commission. We find that the record reflecting these national security and law enforcement risks raises serious concerns as to whether Digitalsystem can be trusted to cooperate with the Committee's mitigation monitoring in good faith and with transparency, and to comply with mitigation terms. Based on our review of the totality of the evidence in the record, we find that Digitalsystem is not likely to cooperate and be fully transparent with the Committee and the Commission in such a way that would allow a mitigation agreement to be effective.

52. Any Commission grant of the pending international section 214 application would need to find that Digitalsystem's provision of global facilities-based and resale common carrier services on U.S.-international routes is in the public interest, convenience, and necessity despite the national security and law enforcement risks identified by the Committee as being unmitigable.[280] Given the evidence in the record, we are persuaded that the underlying foundation of trust that is needed for a mitigation agreement to adequately address national security and law enforcement concerns is not present in the instant case. In this regard, we acknowledge the Committee's established role in monitoring and enforcing compliance with mitigation agreements and, therefore, we conclude that it is appropriate to defer to what we believe to be a reasonable assertion of the Committee that mitigation is not an adequate option here. We therefore conclude, for the purpose of our public interest analysis in this proceeding, that absent the ability to mitigate, any Commission grant of Digitalsystem's application for international section 214 authority would not serve the public interest, convenience, and necessity given the significant national security and law enforcement concerns raised in the record. Therefore, we deny the application.

C. Additional Evidence (Classified)

53. Although our decision to deny Digitalsystem's application for international section 214 authority, and the determination that mitigation will not address the substantial national security and law enforcement risks, would be warranted based solely on the unclassified information in the record, a classified filing provided to the Commission by the Committee provides further support for our decision.

54.

55. [281]

56. [282] [283] [284] [285] [286] [287] [288] [289]

[280] 47 U.S.C § 214; 47 CFR § 63.18.

[281]

[282]

[283]

[284]

[285]

[286]

[287]

[288]

[289]

57. [290] [291]
58. [292]
59. [293]
60. [294] [295] [296]
61.
62. [297] [298]
63. [299] [300] [301]
64.
65. [302] [303] [304]
66. [305]
67.
68. [306] [307]
69.
70.
71. [308] [309]

290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309

72. [310] [311]

73. [312]

74. [313] [314]

75. [315]

76. [316] [317]

77. [318] [319]

78.

79.

80. [320]

81. [321] [322] [323] [324] [325] [326]

82. [327] [328]

83. [329]

84.

85. [330]

86.

310

311

312

313

314

315

316

317

318

319

320

321

322

323

324

325

326

327

328

329

330

87. [331]

88. [332] [333] [334] [335] [336]

89. [337]

90.

91. [338] [339] [340]

92.

93. [341]

94. [342] [343]

95.

96.

97. [344]

98.

IV. ORDERING CLAUSES

99. Accordingly, IT IS ORDERED, pursuant to sections 4(i), 4(j), and 214 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 154(i), (j), 214 and sections 63.12, 63.18, and 63.21, of the Commission's rules, 47 CFR §§ 63.12, 63.18, and 63.21, that the international section 214 authorization application under File No. ITC-214-20240326-00054 IS HEREBY DENIED.

100. IT IS FURTHER ORDERED that a copy of this Memorandum Opinion and Order shall be sent by Certified Mail, Return Receipt Requested, and by regular first-class mail to:[345]

331

332

333

334

335

336

337

338

339

340

341

342

343

344

[345] On April 14 and 15, 2026, the Digitalsystem Letter was mailed via Certified Mail, Return Receipt Requested, and by regular first-class mail to the addresses identified in Digitalsystem's international section 214 application and the address identified in the FCC's Commission Registration System (CORES). On June 18, 2026, the certified letter sent to Hui Xie, CEO of Digitalsystem, at one of the addresses identified in the application (18645 Gale Ave #200 City of Industry, CA 91748) was returned to the FCC. *See* USPS.com, USPS Tracking, Tracking Number 70041160000026196575, https://tools.usps.com/tracking/70041160000026196575 (stating, "Your item was picked (continued….)

Hui Xie, CEO
Digitalsystem Technology Inc
1470 Valley Vista Dr Ste 204
Diamond Bar, CA 91765-3967

Yi Zhou
Digitalsystem Technology Inc
1470 Valley Vista Dr Ste 204
Diamond Bar, CA 91765-3967

Jinze He
Digitalsystem Technology Inc
1470 Valley Vista Dr Ste 204
Diamond Bar, CA 91765-3967

Hui Xie, CEO
Digitalsystem Technology Inc
6 Skyline Ln
Pomona, CA 91766

Alan Xie
Digitalsystem Technology Inc
6 Skyline Ln
Pomona, CA 91766

Yi Zhou
Digitalsystem Technology Inc
6 Skyline Ln
Pomona, CA 91766

101. Petitions for reconsideration under section 1.106 of the Commission's rules, 47 CFR § 1.106, may be filed within 30 days of the date of the release of this Memorandum Opinion and Order.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

up at the post office at 7:56 am on June 18, 2026 in WASHINGTON, DC 20554"). The following notice was attached to the mailing that was returned to the FCC: "Notify Sender of New Address: Digitalsystem Technology Inc., 1470 Valley Vista Dr Ste 204, Diamond Bar, CA 91765-3967." The certified letter sent to one of the addresses identified in the application (6 Skyline Ln, Pomona, CA 91766) was received at that address on April 28, 2026. *See* USPS.com, USPS Tracking, Tracking Number 70041160000026196490), https://tools.usps.com/tracking/70041160000026196490; USPS.com, USPS Tracking, Tracking Number 70041160000026196506, https://tools.usps.com/tracking/70041160000026196506; USPS.com, USPS Tracking, Tracking Number 70041160000026196483, https://tools.usps.com/tracking/70041160000026196483.