PUBLIC NOTICE

Federal Communications Commission
45 L Street NE
Washington, DC 20554

News Media Information 202-418-0500
Internet: www.fcc.gov

DA 26-673
Released: July 7, 2026

FCC'S PUBLIC SAFETY AND HOMELAND SECURITY BUREAU ANNOUNCES ADDITION OF CERTAIN SERVICES OF DIGITALSYSTEM TECHNOLOGY INC. TO FCC COVERED LIST

WC Docket No. 18-89, ET Docket No. 21-232, EA Docket No. 21-233

The Federal Communications Commission's (FCC or Commission) Public Safety and Homeland Security Bureau (PSHSB or Bureau) maintains a list of equipment and services (Covered List) that have been determined to "pose an unacceptable risk to the national security of the United States or the security and safety of United States persons."[1] Pursuant to section 2 of the Secure and Trusted Communications Networks Act of 2019 (Secure Networks Act)[2] and sections 1.50002(a) and 1.50003 of the Commission's rules,[3] PSHSB announces the addition of certain services provided by Digitalsystem Technology Inc. (Digitalsystem) to the Covered List. Specifically, this action applies to Digitalsystem's international telecommunications services that are subject to section 214 of the Communications Act of 1934 (Communications Act). We make this addition to the Covered List based on a determination made by an Executive Branch interagency body with appropriate national security expertise, including appropriate national security agencies.[4]

Specific Determination. On April 3, 2026, the FCC received a recommendation from the Committee for the Assessment of Foreign Participation in the U.S. Telecommunications Services Sector (the Committee) to deny Digitalsystem's application for authorization to provide international telecommunications services under section 214 of the Communications Act (Recommendation). The Committee recommended denying the application due to "the unmitigable and unacceptable risks to the national security and law enforcement interests of the United States."[5] In summary, the Committee

[1] Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601-1609) (Secure Networks Act); 47 CFR §§ 1.50002, 1.50003.

[2] 47 U.S.C. § 1601.

[3] 47 CFR §§ 1.50002(a), 1.50003; *see also Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Second Report and Order, 35 FCC Rcd 14284 (2020) (*Supply Chain Second Report and Order*).

[4] *See* 47 U.S.C. § 1601(c)(1) and (4). The Department of Justice, the Department of Homeland Security, and the Department of War comprise the members of the Committee for the Assessment of Foreign Participation in the U.S. Telecommunications Services Sector (the Committee), formerly known as Team Telecom. *See* Exec. Order No. 13913 of April 4, 2020, 85 Fed. Reg. 19643, Executive Order on Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Apr. 4, 2020). In the *Supply Chain Second Report and Order*, the Commission identified Team Telecom as an executive branch interagency group that routinely provides the Commission with expert national security advice. *See Supply Chain Second Report and Order*, 35 FCC Rcd at 14312-13, para. 61.

[5] 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, at 6 (filed Apr. 2, 2026). (Committee

determined that: (1) the services that Digitalsystem is seeking to provide pose risks to the United States because they could be exploited by the PRC and Hong Kong-based threat actors to the detriment of U.S. interests; (2) Digitalsystem's planned service offerings, proposed partnerships, and existing and potential relationships with service providers exacerbate these risks; and (3) mitigation measures are infeasible in light of the inconsistent and changing responses by Digitalsystem, which undermine the candor and reliability required of any national-security mitigation partner, and Digitalsystem's business plans.[6] After reviewing this Recommendation and allowing Digitalsystem an opportunity to respond, the Commission denied Digitalsystem's application, agreeing with the Committee that, among other things, foreign adversary control of Digitalsystem posed "substantial and unacceptable national security and law enforcement risks."[7]

The Covered List. We find that the Recommendation constitutes a "specific determination" that Digitalsystem's international telecommunications services "pose an unacceptable risk to the national security of the United States or the security and safety of United States persons" pursuant to section 2 of the Secure Networks Act.[8] Therefore, we conclude that the Commission is required to place the services in this determination on the Covered List.[9] We update the Covered List to include:

> "International telecommunications services provided by Digitalsystem Technology Inc., subject to section 214 of the Communications Act of 1934."

The inclusion of these services on the Covered List extends to services of subsidiaries and affiliates of Digitalsystem.

The updated Covered List is attached as Appendix A to this Public Notice and is published on the Bureau's website at https://www.fcc.gov/supplychain/coveredlist.[10] The list of devices that have been granted Conditional Approvals is available at https://www.fcc.gov/supplychain/coveredlist#conditional-approvals. The Recommendation is attached as Appendix B to this Public Notice.

For further information, please contact Chris Smeenk at Chris.Smeenk@fcc.gov or 202-418-1630, or Rebecca Clinton at Rebecca.Clinton@fcc.gov or 202-418-7815, Attorney Advisors, Operations and Emergency Management Division, Public Safety and Homeland Security Bureau.

Recommendation). The Committee Recommendation is available via the International Communications Filing System (ICFS) by searching for ITC-214-20240326-00054 and accessing "Pleadings & Comments."

[6] Committee Recommendation at 28; s*ee also id.* at 1-2.

[7] *Digitalsystem Technology Inc. Application for Global Facilities-Based and Global Resale International Telecommunications Authority Pursuant to Section 214 of the Communications Act of 1934, as Amended*, ITC-214-20240326-00054, Memorandum Opinion and Order, FCC 26-44, para. 16 (Jul. 7, 2026).

[8] 47 U.S.C. § 1601(c).

[9] 47 U.S.C. § 1601(b)-(d).

[10] The FCC website also contains a list of certain affiliates and subsidiaries of entities identified on the Covered List. The list of affiliates and subsidiaries does not constitute a comprehensive list of all entities that the Commission may find, upon further examination, to qualify as relevant subsidiaries or affiliates of entities on the Covered List. Those entities, whether or not they currently provide covered communications equipment or services, are subject to the Commission's prohibitions, such as the prohibition against obtaining authorizations for covered equipment. *See Reminder: Communications Equipment And Services On The Covered List Pose An Unacceptable Risk To National Security*, National Security Advisory No. 2025-01, DA 25-927, note 3 (PSHSB Oct. 14, 2025).

APPENDIX A

COVERED LIST (Updated July 7, 2026)*†±

Covered Equipment or Services*	Date of Inclusion on Covered List
Telecommunications equipment produced or provided by **Huawei Technologies Company**, including telecommunications or video surveillance services produced or provided by such entity or using such equipment.	March 12, 2021
Telecommunications equipment produced or provided by **ZTE Corporation**, including telecommunications or video surveillance services provided or provided by such entity or using such equipment.	March 12, 2021
Video surveillance and telecommunications equipment produced or provided by **Hytera Communications Corporation**, to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services produced or provided by such entity or using such equipment.	March 12, 2021
Video surveillance and telecommunications equipment produced or provided by **Hangzhou Hikvision Digital Technology Company**, to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services produced or provided by such entity or using such equipment.	March 12, 2021
Video surveillance and telecommunications equipment produced or provided by **Dahua Technology Company**, to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services produced or provided by such entity or using such equipment.	March 12, 2021
Information security products, solutions, and services supplied, directly or indirectly, by **AO Kaspersky Lab** or any of its predecessors, successors, parents, subsidiaries, or affiliates.	March 25, 2022
International telecommunications services provided by **China Mobile International USA Inc.** subject to section 214 of the Communications Act of 1934.	March 25, 2022
Telecommunications services provided by **China Telecom (Americas) Corp.** subject to section 214 of the Communications Act of 1934.	March 25, 2022
International telecommunications services provided by **Pacific Networks Corp.** and its wholly-owned subsidiary **ComNet (USA) LLC** subject to section 214 of the Communications Act of 1934.	September 20, 2022
International telecommunications services provided by **China Unicom (Americas) Operations Limited** subject to section 214 of the Communications Act of 1934.	September 20, 2022
Cybersecurity and anti-virus software produced or provided by **Kaspersky Lab, Inc.** or any of its successors and assignees.	July 23, 2024
Uncrewed aircraft systems (UAS) and UAS critical components produced in a foreign country††—except: (a) UAS and UAS critical components included on the Defense Contract Management Agency's (DCMA's) Blue UAS Cleared List, until January 1, 2027;# (b) UAS and UAS critical components that qualify as "domestic end products" under the Buy American Standard, 48 CFR 25.101(a), until January 1, 2027; (c) devices which have been granted a Conditional Approval by DoW or DHS; and (d) foreign-produced "Toy Drones," as defined in the National Security Determination, and "Toy Drones that contain foreign-produced components." All communications and video surveillance equipment and services listed in Section 1709(a)(1) of the FY25 National Defense Authorization Act (Pub. L. 118-159).	December 22, 2025 Updated: January 7, 2026 Updated: March 18, 2026 Updated: June 15, 2026
Routers^ produced in a foreign country, except routers which have been granted a Conditional Approval by DoW or DHS.	March 23, 2026
International telecommunications services provided by **Digitalsystem Technology Inc.**, subject to section 214 of the Communications Act of 1934.	July 7, 2026

*The inclusion of producers or providers of equipment or services named on this list should be read to include the subsidiaries and affiliates of such entities.

†Where equipment or services on the list are identified by category, such category should be construed to include only equipment or services capable of the functions outlined in sections 2(b)(2)(A), (B), or (C) of the Secure and Trusted Communications Networks Act of 2019, 47 U.S.C. § 1601(b)(2)(A)-(C).

††For purposes of inclusion of UAS and UAS critical components, we incorporate the definitions included in the associated National Security Determination.

±The scope of the Covered List is affected by the Conditional Approvals that we have received.

#The "Blue UAS list" referred to in the National Security Determination is the combination of the "Blue UAS Cleared List" at https://bluelist.appsplatformportals.us/Cleared-List/ and the list of compliant UAS components and software at https://bluelist.appsplatformportals.us/Framework/. We use the term "Blue UAS Cleared List" to refer to both lists.

^For purposes of inclusion of routers, we incorporate the definitions included in the associated National Security Determination

APPENDIX B

Recommendation of the Committee for the Assessment of Foreign Participation in the U.S. Telecommunications Services Sector to Deny the Application
April 1, 2026

[[FOR PUBLIC INSPECTION; E.O. 13913 CONFIDENTIAL INFORMATION REDACTED]]

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of DIGITALSYSTEM TECHNOLOGY INC. Application for authority under Section 214 of the Communications Act of 1934, as amended, to provide facilities-based and resold telecommunications services in accordance with 47 C.F.R. §§ 63.12 and 63.18	File No. ITC-214-20240326-00054

Recommendation of the Committee for the Assessment of Foreign Participation in the U.S. Telecommunications Services Sector to Deny the Application

[[FOR PUBLIC INSPECTION; E.O. 13913 CONFIDENTIAL INFORMATION REDACTED]]

TABLE OF CONTENTS

[[FOR PUBLIC INSPECTION; E.O. 13913 CONFIDENTIAL INFORMATION REDACTED]]

further eroded the trust required of a national-security mitigation partner. Throughout the review, Digitalsystem provided conflicting, incomplete, and/or misleading responses on multiple topics of importance to the Committee's analysis, which raise doubts about Digitalsystem's truthfulness and ability to engage in a productive compliance relationship. These topics include Digitalsystem's plans to provide services to **[BEGIN CONFID. INFO] [END CONFID. INFO]**, Digitalsystem's partnerships with **[BEGIN CONFID. INFO] [END CONFID. INFO]**, the extent of Digitalsystem's owners' access to company records and systems, the type and extent of other access by foreign individuals and entities to Digitalsystem's U.S. records, data, and equipment, and Digitalsystem's lawful intercept capabilities. These concerns are further exacerbated by significant vulnerabilities presented by Digitalsystem's planned business, including not only partnership with **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

If Digitalsystem held an international Section 214 authorization and threat actors based in mainland China, Hong Kong, or elsewhere were to exploit Digitalsystem, there would be significant negative consequences for U.S. national security and law enforcement interests. Namely, threat actors could collect or exfiltrate U.S. communications content and sensitive U.S. records, disrupt U.S. communications, misroute U.S. communications to jurisdictions of concern, or expose sensitive U.S. law enforcement information. The FCC should deny the application.

II. Legal Authority

A. The FCC's Authority Over Section 214 Authorizations

Under section 214 of the Communications Act of 1934, no telecommunications carrier may provide service over domestic or international transmission lines until the FCC certifies that such services will serve the public interest.[3] The FCC has "wide discretion" in determining whether a license would advance the public interest,[4] and a "crucial factor" is "whether a carrier's use of domestic or international transmission lines raises any national security, law enforcement, or foreign policy concerns."[5]

B. The Committee's Role

Under Executive Order 13913 ("E.O. 13913"), the Department of Justice ("DOJ"), the Department of Homeland Security, and the Department of War comprise the Members of the Committee, whose primary objective is to assist the

[3] 47 U.S.C. § 214(a); 47 C.F.R. § 63.18.

[4] *FCC v. RCA Comm'cns, Inc.*, 346 U.S. 86 90 (1953).

[5] *China Telecom (Ams.) Corp. v. FCC*, 57 F.4th 256 261 (D.C. Cir. 2022).

[[FOR PUBLIC INSPECTION; E.O. 13913 CONFIDENTIAL INFORMATION REDACTED]]

FCC in its public-interest review of national security and law enforcement concerns that may be raised by foreign participation in the U.S. telecommunications services sector.[6] The Committee reviews applications referred by the FCC for risks to U.S. national security and law enforcement interests. Based on its review, the Committee advises the FCC on the disposition of the application—non-objection to granting the application, a recommendation that the FCC only grant the license contingent on the applicant's compliance with mitigation measures to address the risks identified, or a recommendation that the FCC deny the application due to the risk to the national security or law enforcement interests of the United States where such risks cannot be mitigated.[7]

The FCC has long treated national security and law enforcement concerns as important public interest factors in the advice that the FCC seeks from other Executive Branch agencies.[8] The FCC will "accord deference to the expertise of Executive Branch agencies in identifying and interpreting issues of concern related to national security, law enforcement, and foreign policy."[9] This advice "must occur only after appropriate coordination among Executive Branch agencies, must be communicated in writing, and will be part of the public file in the relevant

---

6 Exec. Order No. 13,913 §§ 3(a); 3(b), 85 Fed. Reg. 19,643 (Apr. 8, 2020).

7 *Id.* at 19,646; 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 & 95-22, Report and Order and Order on Reconsideration, 12 FCC Rcd 23891, 23919–20, ¶ 61 (1997) (hereinafter "1997 Foreign Participation Order") (noting that the FCC will "continue to find national security, law enforcement, foreign policy, and trade policy concerns relevant to our decision to grant or deny Section 214 … applications.)" and that the FCC's public interest analysis "would benefit from input by the Executive Branch addressing these issues."); *see also id.* at n.252 (noting that the FCC's analysis under Section 2 of that Act includes "discretion to deny an application if to do so would . . . 'promote the security of the United States'"); *Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership*, IB Docket No. 16-155, FCC 20-133, Report and Order, 35 FCC Rcd 10,927 (Oct. 1, 2020) (hereinafter "Executive Branch Review Order") (adopting rules and procedures to streamline and improve the efficiency and transparency of the process by which the FCC coordinates with Executive Branch agencies for assessment of any national security, law enforcement, foreign policy, and/or trade policy issues related to certain applications filed with the FCC).

8 *1997 Foreign Participation Order*, 12 FCC Rcd at 23,919–20, ¶¶ 62–63; *see also Executive Branch Review Order*, 35 FCC Rcd at 10,928–31, ¶¶ 3–7.

9 *1997 Foreign Participation Order*, 12 FCC Rcd at 23,920, ¶ 63; *see also* Reform of Rules and Policies on Foreign Carrier Entry into the U.S. Telecommunications Market, Report and Order, 29 FCC Rcd 4256, 4258, ¶ 4 (2014) (hereinafter "2014 Foreign Carrier Entry Order") ("The [FCC]'s presumption, however, is limited to competition issues; it does not apply to questions regarding national security, law enforcement, foreign policy or trade policy concerns, and such questions are resolved in the same manner regardless of the WTO status of the carrier's home country. The [FCC] accords deference to Executive Branch agencies in identifying and interpreting issues of concern related to these matters."); *Telefonica Puerto Rico*, 12 FCC Rcd at 5,182–85 ¶¶ 24–33 (adopting the State Department's disapproval of a proposed cable application, in coordination with the advice of the Department of Defense, NTIA, and USTR, and noting State Department's determination that "grant of the applications would be inconsistent with the rights and interests of U.S. companies that desire to compete in the Spanish telecommunications market").

[[FOR PUBLIC INSPECTION; E.O. 13913 CONFIDENTIAL INFORMATION REDACTED]]

proceeding."[10] While ultimately making its own independent decision, the FCC "accord[s] deference" to the Committee's (and its predecessor's) expertise in these issues,[11] and the D.C. Circuit has likewise recognized "the deference [it] owe[s] to the Executive Branch agencies' recommendations and the Commission's judgment."[12]

E.O. 13913 established formal processes for the Committee to follow in reviewing applications (including for international Section 214 authorizations) for national security and law enforcement concerns.[13] If the Committee decides to recommend that the FCC deny an application, the Committee must first notify the Committee Advisors and consult them on their views as to the recommendation.[14] The Committee Advisors have 21 days to advise the Chair whether they oppose the recommendation; if a Committee Advisor does so, then the Committee and the Advisors follow the process established under E.O. 13913 to try resolve any opposition and reach consensus.[15] If there is no opposition, the Committee provides its recommendation to the FCC.

III. Background on This International Section 214 Application

A. Applicant and FCC Application

Digitalsystem, a California business, is a **[BEGIN CONFID. INFO] [END CONFID. INFO]** company seeking an international 214 authorization to provide telecommunications services to international locations **[BEGIN CONFID. INFO] [END CONFID. INFO]**. Digitalsystem is 70% directly owned by Hui Xie **[BEGIN CONFID. INFO] [END CONFID. INFO]**, a Chinese citizen **[BEGIN CONFID. INFO] [END CONFID. INFO]**, and 30% directly owned by Yi Zhou **[BEGIN CONFID. INFO] [END CONFID. INFO]**, a U.S. citizen **[BEGIN CONFID. INFO] [END CONFID. INFO]**[16] **[BEGIN CONFID. INFO] [END CONFID.**

---

[10] *1997 Foreign Participation Order*, 12 FCC Rcd at 23,921, ¶ 66; *see also id.* at n.121 ("To the extent the Executive Branch must share classified information with [FCC] staff, such information is not subject to public disclosure").

[11] *E.g.*, *id.* at ¶¶ 61–63 (1997).

[12] *China Telecom (Americas) Corp.*, 57 F.4th at 267.

[13] *See generally* E.O. 13913, 85 Fed. Reg. 19,643 (Apr. 8, 2020).

[14] *Id.* at 19,647. The Committee Advisors consist of the Secretary of State, Secretary of the Treasury, Secretary of Commerce, Director of the Office of Management & Budget, United States Trade Representative, Director of National Intelligence, Administrator of General Services, Assistant to the President for National Security Affairs, Assistant to the President for Economic Policy, Director of the Office of Science and Technology Policy, and the Chair of the Council of Economic Advisors (plus any other Assistants to the President that the President designates). *Id.* at 19,644.

[15] *See id.* at 19,647.

[16] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

[[FOR PUBLIC INSPECTION; E.O. 13913 CONFIDENTIAL INFORMATION REDACTED]]

INFO].[17] Digitalsystem stated that it is **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[18] At the time it submitted responses to the Committee's questions, Digitalsystem stated that it had **[BEGIN CONFID. INFO] [END CONFID. INFO]** employees, but may hire **[BEGIN CONFID. INFO] [END CONFID. INFO]** employees as the business grows.[19]

Digitalsystem is applying for a new international Section 214 authorization to provide global facilities-based and resold services.[20] Digitalsystem is an existing company specializing in **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[21]

Currently, **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[22] Digitalsystem also stated that it currently has **[BEGIN CONFID. INFO] [END CONFID. INFO]** customers for telecommunications services, **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[23] Digitalsystem explained that it is seeking the international Section 214 authorization to expand its international telecommunications connectivity so that it can directly provide **[BEGIN CONFID. INFO] [END CONFID. INFO]** as well as expand its service scope to provide **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[24]

B. Digitalsystem's Related Global Operations

Though a U.S. company, Digitalsystem is affiliated with several international "sister companies," including one based in Hong Kong. **[BEGIN CONFID. INFO] [END CONFID. INFO]**. Specifically, Digitalsystem has related independent companies in Hong Kong (Digital Hongkong Technology Ltd.), Mexico (ICT System SA DE CV), and Brazil (Digitalsystem Technology Inc. Ltda.).[25] Digitalsystem stated that these companies are **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[26] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[27]

Further, while Digitalsystem originally stated **[BEGIN CONFID. INFO] [END CONFID. INFO]**. Digitalsystem explained that **[BEGIN CONFID. INFO]**

---

17 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

18 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

19 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

20 FCC File No. ITC-214-20240326-00054.

21 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

22 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

23 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

24 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

25 **[BEGIN CONFID. INFO] [END CONFID. INFO]**; *see also Connect with Us*, Digitalsystem (last visited Feb. 27, 2026), https://www.digitalsystem.net/about.html.

26 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

27 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

[[FOR PUBLIC INSPECTION; E.O. 13913 CONFIDENTIAL INFORMATION REDACTED]]

[END CONFID. INFO].[28] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[29] Digitalsystem stated that **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[30]

Digitalsystem described **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[31] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

IV. Procedural Background

The Applicant filed its application with the FCC on March 26, 2024. The FCC referred the application to the Committee on June 14, 2024. The Committee notified the FCC that the Applicant's triage responses were complete on June 30, 2025, starting the 120-day initial review period. Unusually, as explained in more detail below, it took approximately a year for the Committee to certify completeness of the Applicant's responses in this case because the Applicant's responses were frequently inconsistent, ambiguous, and incomplete, requiring multiple rounds of follow-up and re-submission by the Applicant.

On December 10, 2025, the Committee notified the FCC of its determination that a secondary assessment of the application was warranted because the risk to national security or law enforcement interests cannot be mitigated by standard mitigation measures.[32] The Committee notified the Committee Advisors on February 23, 2026 of its determination to recommend that the FCC deny the application, beginning the 21-day period for the Advisors to oppose the recommendation.[33]

V. The Committee Recommends Denying the Application

The Committee recommends denying the application due to the unmitigable and unacceptable risks to the national security and law enforcement interests of the United States.

A. The Government of the PRC is a foreign adversary that poses a national security threat to the United States within the context of this application.

---

28 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

29 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

30 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

31 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

32 *See* E.O. 13913 §§ 5(b), (c).

33 *See id.* § 9(f).

[[FOR PUBLIC INSPECTION; E.O. 13913 CONFIDENTIAL INFORMATION REDACTED]]

1. The Government of the PRC presents a significant counterintelligence threat to the United States.

The United States has long recognized that the Chinese government is a national security threat to the United States. According to ODNI, the PRC remains the "most active and persistent cyber threat to U.S. government, private sector, and critical infrastructure networks."[34] The PRC's cyber-espionage operations have included "compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations."[35] The PRC has also conducted cyber operations against U.S. critical infrastructure that appear to have been intended to pre-position the PRC to disrupt U.S. communications if there is a conflict between the United States and the PRC.[36]

The PRC government uses its own agencies and government-controlled companies to engage in espionage and other activities that compromise U.S. national security. The U.S. government considers the PRC to be a "foreign adversary" because of its long-term pattern of engagement in economic and traditional espionage to acquire U.S. technology, intellectual property ("IP"), and U.S. persons' sensitive personal data.[37] For more than a decade, the PRC has executed a comprehensive, long-term industrial strategy against the United States and other countries to advance its economic, military, and national security interests, including through exploitation of the U.S. information and communications technology or services supply chain. As part of this strategy, the PRC has integrated its technological ambitions into a broader government-directed approach to acquire technology and IP the PRC deems critical to its industrial growth and military modernization plans.[38] The

---

[34] Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community 11 (Mar. 18, 2025).

[35] Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community (Feb. 6, 2023).

[36] Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community 11 (Feb. 5, 2024).

[37] *See* Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. 4,923, 4,925, § 7.4 (defining the PRC, including Hong Kong, as a "foreign adversary" due to its "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," pursuant to Executive Order 13873, *Security the Information Communications Technology and Services Supply Chain* (May 15, 2019)).

[38] *See, e.g.*, U.S. DEP'T OF STATE, *Report to Congress on U.S.-Origin Technology that the Chinese Communist Party (CCP) is Using in the Military Civil Fusion (MCF) Strategy of the PRC* 2–3 (Aug. 27, 2025), https://www.state.gov/wp-content/uploads/2025/08/Report-U.S.-Technology-in-the-Military-Civil-Fusion-Strategy-Revision-Accessible-8.27.2025.pdf:

> MCF leverages and exploits civilian access to international technology, investments, research and development (R&D), and partnerships to develop the PRC's civilian, military, and intelligence capabilities .... The PRC seeks and obtains foreign technology and intellectual

[[FOR PUBLIC INSPECTION; E.O. 13913 CONFIDENTIAL INFORMATION REDACTED]]

PRC's ultimate goal is to secure global dominance in key industrial sectors and to develop the most technologically advanced military in the world through the large-scale transfer of targeted foreign technologies. However, unlike other developed, rule-of-law based countries, the PRC pursues these goals through malign behaviors ranging from the facially legal to the illicit, including various forms of economic espionage, forced technology transfer, strategic acquisitions, and other less obvious tactics to advance its economic and military development at the United States' expense.[39]

While there are many examples of PRC-linked cyberattacks in the United States, three recent cyberattacks demonstrate some of tactics the PRC has employed against U.S. companies, including telecommunications companies. PRC cyber actors known as "Salt Typhoon" are reportedly responsible for the compromise of U.S. telecommunications companies publicly reported in October 2024. Salt Typhoon is being investigated for "attacking telecommunications companies, stealing customer information and law enforcement information, and targeting political figures."[40] PRC-linked actors known as "Volt Typhoon" have targeted U.S. critical infrastructure entities, employing "living off the land" techniques to use built-in tools on target networks to execute objectives without installing malware that could be more easily detected by victim entities.[41] Finally, "Flax Typhoon" are actors associated with PRC information security companies that take direction from the PRC government and have targeted U.S. critical infrastructure and Taiwanese entities in the United States and abroad.[42] Flax Typhoon has also used living-off-the-land techniques and has "compromised hundreds of internet of things ("IOT") devices to create a botnet that they use to carry out attacks."[43]

The PRC's legal regime also presents significant national security concerns. Overall:

> China has enacted the world's most comprehensive set of laws, regulations, and national plans to broadly define its national and public security interests in data and to govern data collection, sales, sharing, and storage. This regime provides the PRC with broad control of large datasets

---

property as well as nascent intellectual capital through a variety of means, including foreign direct investment; overseas acquisitions; technology imports; the establishment of foreign R&D centers, joint ventures, research and academic partnerships; talent recruitment; and industrial and cyber espionage.

39 *Id.*

40 Chris Jaikaran, CONG. RESEARCH SERVICE, *Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications* (Jan. 23, 2025), https://www.congress.gov/crs-product/IF12798.

41 *Id.*

42 *Id.*

43 *Id.*

[[FOR PUBLIC INSPECTION; E.O. 13913 CONFIDENTIAL INFORMATION REDACTED]]

> hosted in China—controlled by both Chinese and non-Chinese companies—allowing it to restrict and suppress data that it deems could harm its national security or benefit international competitors.[44]

For example, the 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."[45] 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."[46] PRC citizens or companies that oppose requests from PRC intelligence or security services do not have adequate legal recourse to challenge such requests.[47]

The PRC's 2017 National Intelligence Law similarly authorizes "national

---

[44] *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 ¶ 16, *TikTok Inc.* v. *Garland*, Case Nos. 24-1113, 24-1130, 24-1183 (D.C. Cir. July 26, 2024) (publicly filed redacted version) (hereinafter "Newman Decl.").

[45] *Id.* at ¶ 19 (quoting a translation of the National Security Law of the People's Republic of China, promulgated by the Standing Committee of the National People's Congress, July 1, 2015, effective July 1, 2015). The law broadly defines national security as "the state where the country's political power, sovereignty, unity and territorial integrity, people's wellbeing, sustainable economic and social development, and other major national interests are relatively free from danger and internal and external threats" and "the ability to maintain a continuous state of security." *Id.*

[46] *Id.* at ¶ 20 (emphasis added) (quoting a translation of the Cybersecurity Law of the People's Republic of China, promulgated by the Standing Committee of the National People's Congress, Nov. 7, 2016, effective June 1, 2017).

[47] *See* 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 ("There is also a deep bench of expansively-worded Chinese laws that require cooperation with state officials in virtually all matters, a heavy-handed security apparatus in no way shy about using such coercive tools, and a Party-run judicial system that precludes effective legal recourse to anyone with whom the Chinese Communist Party disagrees."); *see generally* U.S. DEP'T OF STATE, China Country Report on Human Rights Practices for 2019 14 (2020) ("Although the law states the courts shall exercise judicial power independently, without interference from administrative organs, social organizations, and individuals, the judiciary did not exercise judicial power independently. Judges regularly received political guidance on pending cases, including instructions on how to rule, from both the government and the CCP, particularly in politically sensitive cases.").

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."[48] This law gives PRC intelligence services greater powers to compel Chinese citizens and organizations "to cooperate, assist, and support Chinese intelligence efforts *wherever they are in the world*."[49] 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.[50] The PRC uses these comprehensive laws to "effectively blur[] the line between the private and public sector," making it so that "Chinese companies lack meaningful independence from the PRC's agenda and objectives."[51]

A group of laws passed in 2020 and 2021 also increase the threat from the PRC; these laws include: the Cyber Vulnerability Reporting Law, Personal Information Protection Law, Anti-Foreign Sanctions Law, and Data Security Law. 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.[52] Similarly expanding state power and access, the Cyber Vulnerability Reporting Law was implemented by the Cyberspace Administration of China, the Ministry of Public Security, and the Ministry of Industry and

---

[48] Newman Decl., at ¶ 22 (quoting a translation of the National Intelligence Law of the People's Republic of China, promulgated by the Standing Committee of the National People's Congress, June 27, 2017, effective June 28, 2017, amended Apr. 27, 2018).

[49] *See China Mobile Int'l, Inc.*, 34 FCC Rcd. 3361 (4) at 9 ¶ 17 (emphasis added). The FCC's *China Mobile* Order noted at ¶ 17 & nn. 55–5 that:

> Article 7 of the 2017 National Intelligence Law provides 'an 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.' Article 14 permits Chinese intelligence institutions to request citizens and organizations to provide necessary support, assistance, and cooperation. Article 17 allows Chinese intelligence agencies to take control of an organization's facilities, including communications equipment.[49]

[50] Newman Decl., at ¶ 23 (quoting a translation of the Counter-Espionage Law of the People's Republic of China, promulgated by the Standing Committee of the National People's Congress, Nov. 1, 2014, amended Apr. 26, 2023, effective July 1, 2023).

[51] *Id.* at ¶ 25, 17.

[52] *See* 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* (Dec. 22, 2020), https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf at 7–8.

[[FOR PUBLIC INSPECTION; E.O. 13913 CONFIDENTIAL INFORMATION REDACTED]]

Information Technology ("MIIT"), which published the "Regulations on the Management of Network Product Security Vulnerabilities" ("RMSV"), in July 2021.[53] These regulations require any business operating in the PRC to report software vulnerabilities to MIIT within forty-eight hours of their discovery. The rules prohibit researchers from: "publishing information about vulnerabilities before a patch is available, unless they coordinate with the product owner and the MIIT; publishing proof-of-concept code used to show how to exploit a vulnerability; and exaggerating the severity of a vulnerability."[54] In effect, the regulations push all software-vulnerability reports to MIIT before a patch is available.

Concurrent to the implementation of this new rule, Microsoft's "Digital Defense Report 2022" showed a corresponding uptick in the number of zero-day vulnerabilities deployed by PRC-based hacking groups. Microsoft explicitly attributes the increase as a "likely" result of the RMSV. Finally, in 2023, Atlantic Council researchers found that the RMSV allows the PRC government, and subsequently the Ministry of State Security, to access vulnerabilities previously uncaptured by past regulatory regimes and policies. In some cases, the regulations also facilitate access to some companies' internal code repositories. The mandated vulnerability and threat-intelligence sharing within PRC agencies allows access to reporting by a regional PRC Ministry for State Security ("MSS") office, a known People's Liberation Army ("PLA") contractor, and a university research center with ties to PLA hacking campaigns and which conducts offensive and defense research.[55] The MSS has been linked to hacking campaigns against U.S. persons, enterprises, and government for purposes of transnational repression and cyber and economic espionage.[56]

The PRC has continued to expand its authority in more recent years. In April 2023, the PRC revised its 2014 Counter-Espionage Law and expanded the scope of espionage activities to broadly include, among other activities:

> theft, espionage, purchase, or illegal provision of national secrets, intelligence, and other documents, data, materials, and items related to national security and interests, carried out by foreign institutions, organizations, or individuals other than espionage organizations and their agents, or directed, funded, or colluded in by such entities,

---

53 Dakota Cary and Kristin Del Ross, ATLANTIC COUNCIL, *Sleight of Hand: How China Weaponizes Software Vulnerabilities* (Sept. 6, 2023), https://www.atlanticcouncil.org/in-depth-research-reports/report/sleight-of-hand-how-china-weaponizes-software-vulnerability/.

54 *Id.*

55 *Id.*

56 USDOJ Press Release: Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians (Mar. 25, 2024).

> or activities aimed at inciting, enticing, coercing, or bribing state employees to betray.[57]

Like the National Intelligence Law, the revised 2023 Counterespionage Law explicitly requires "[a]ll citizens and organizations" to "support and assist in counter-espionage work."[58] The law requires all organizations in the PRC to bear responsibility for counterespionage work, and expands the toolboxes of national security agencies to investigate espionage-related matters.[59] The PRC revised its States Secrets law in 2024 for the first time since 2010, expanding the powers for the police to conduct investigations into breaches and require private companies to take steps to protect "state secrets."[60]

Courts 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.[61] The result is no different here. The increasing breadth and vagueness of

---

[57] Newman Decl., at Ex. E (translation of the Counter-Espionage Law of the People's Republic of China, promulgated by the Standing Committee of the National People's Congress, Nov. 1, 2014, amended Apr. 26, 2023, effective July 1, 2023, by the Xinhua News Agency (Apr. 27, 2023) at Art. 4(3).

[58] *Id.* at Ex. E, Art.8.

[59] *See, e.g., id.* at Ex. E, Arts. 12, 17–21.

[60] Laurie Chen, REUTERS, *China Details Expanded Law on State Secrets, Eyeing Data* (July 24, 2024), reuters.com/world/china/china-details-expanded-law-state-secrets-eyeing-data-security-2024-07-24.

[61] *See China Unicom (Ams.) Operations Ltd. v. FCC*, 124 F.4th 1128, 1152 (9th Cir. 2024) (finding that the FCC properly concluded that there are significant national-security concerns that Chinese cybersecurity and intelligence laws "could require Chinese companies, including CUA's indirect parents, to assist the Chinese government's intelligence-collection efforts" and noting the CUA's connections to Hong Kong—including the storage of customer records in Hong Kong, the use of a network operation center in Hong Kong, and the ability to reconfigure the network remotely from Hong Kong, supported the revocation of CUA's Section 214 authorization); *see also, e.g., China Telecom (Ams.) Corp.*, 57 F.4th 246, 263–65 (finding that the FCC's Revocation Order of China Telecom (Americas) Corporation's Section 214 authorization was supported by "reasoned decisionmaking and substantial evidence in the unclassified record," including the Executive Branch's assessment that "China has augmented the level of state control over the cyber practices of Chinese companies," in part through its national security laws); *Pac. Networks Corp. v. FCC*, 77 F.4th 1160, 1164 (D.C. Cir. 2023) (citing the FCC's and Executive Branch's analysis that a Chinese law requiring Chinese corporations to "support, assist, and cooperate with national intelligence efforts" supported the revocation of Section 214 authorizations based on national-security risk); *TikTok Inc. & ByteDance Ltd. v. Garland*, 122 F.4th 930, 954 (D.C. Cir. 2024) (deferring to the Government's judgement that Chinese laws, including the PRC's National Security Law of 2015 and Cybersecurity Law of 2017 mean that "'even putatively 'private' companies based in China do not operate with independence from the government'" and that the PRC can "'conduct espionage, technology transfer, data collection, and other disruptive activities under the disguise of an otherwise legitimate commercial activity.'" The Supreme Court upheld the D.C. Circuit's judgement in favor of the government in *TikTok v. Garland*, 604 U.S. 56 (2025); *see, e.g., id.* at 74–75, citing H.R. Rep. at 4 ("Chinese law enables China to require companies to surrender data to the

the PRC's laws regarding national security and data security threaten the sensitive information of even private businesses, with little recourse available in the PRC to challenge government action.

2. The relationship between the PRC and Hong Kong presents risks to U.S. national security and law enforcement interests through this application.

Digitalsystem's plans to provide services to and from **[BEGIN CONFID. INFO] [END CONFID. INFO]**, presents 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.[62] Even as early as 2020, the Committee recognized the unacceptable risks posed by the PRC's legal regime as applied to entities and telecommunications infrastructure located in Hong Kong in recommending the partial denial of a subsea-cable application because of the proposed transmission through Hong Kong territory and a Hong Kong-based owner.[63] The FCC's 2022 Order revoking China Unicom (Americas)'s Section 214 authorization echoed these concerns, noting—in reliance on Committee analysis—that the PRC's legal regime "enhances the Chinese government's ability to access information 'entering Chinese territory or traveling through Chinese-owned or -controlled infrastructure *outside of China*,'" namely, in Hong Kong.[64]

The progression of the Beijing-Hong Kong relationship since the mid-1980s demonstrates how mainland China's increasing exertion of control over Hong Kong has eroded Hong Kong's autonomy, especially in relation to national security and law enforcement matters. In accordance with the 1984 China-United Kingdom Joint Declaration, the PRC pledged that Hong Kong would continue to have autonomy except for foreign affairs and defense, and maintain independent

government, 'making companies headquartered there an espionage tool' of China").

62 Exec. Order No. 13,936, 85 Fed. Reg. 43,413 (July 14, 2020) (hereinafter "E.O. 13936"); *see also id., 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.").

63 *See* Executive Branch Recommendation for a Partial Denial and Partial Grant of the Application for a Submarine Cable Landing License for the Pacific Light Cable Network (hereinafter "Executive Branch PLCN Recommendation"), *In the Matter of GU Holdings Inc., Edge Cable Holdings USA, LLC and Pacific Light Data Communication Co. Ltd.*, File Nos. SCL-LIC-20170421-00012; SCL-AMD-20171227-00025; SCL-STA-20180907-00033; SCL-STA-20190327-00011; SCL-STA-20190906-00032; SCL-STA-20200129-00006; SCL-STA-20200313-00014, SCL-STA-20200402-00015 (June 17, 2020).

64 *See China Unicom (Americas) Ops. Ltd.*, FCC File Nos. ITC-214-20020728-00361, ITC-214-20020724-00427, GN Docket No. 20-110, Order on Revocation, FCC 22-9 (Feb. 2, 2022), https://www.fcc.gov/document/china-unicom-americas-order-revocation (hereinafter "China Unicom FCC Revocation Order") at ¶68 (emphasis added) (citing Executive Branch PLCN Recommendation at 24, 26–28).

executive, legislative, and judicial powers. Hong Kong and the central government of China operated under this "one country, two systems" policy since 1990, with Hong Kong operating under its own Basic Law constitutional document. This document codified the PRC's commitment to the two-system policy for a period of 50 years, with the PRC obtaining sovereignty over the Hong Kong Special Administrative Region ("HKSAR") from the United Kingdom in 1997. However, decisions and actions by the PRC central government and the Hong Kong government have brought the fidelity of the two-system arrangement under scrutiny in recent years, raising concerns over whether Hong Kong is operating independent of the PRC central government.[65]

In 2015, the PRC announced its Digital Silk Road ("DSR") plan to extend China's digital infrastructure, technology, and digital influence.[66] In 2019, the Hong Kong Trade Development Council—a statutory body established by the Hong Kong Government in 1966 to create opportunities for business in the region—published an article detailing the important role Hong Kong plays in the DSR plan as a critical economic and geographic hub for the PRC.[67] In 2020, the PRC imposed the National Security Law ("NSL") over the HKSAR. The NSL made structural changes to the relationship between Hong Kong and enabled the PRC central government to assert greater control over the region.[68] The NSL codified four offenses: secession, subversion, terrorist activities, and collusion with foreign countries and external elements, though these offenses are very broadly defined, leaving a large amount of discretion to the PRC and Hong Kong governments to determine what is covered.[69] These legal changes—as well as a "series of actions that have increasingly denied autonomy and freedoms that China promised to the people of Hong Kong under the [1984 China-United Kingdom Joint Declaration]"—led to President Trump's 2020 Executive Order eliminating different and preferential treatment for Hong Kong, in the interest of U.S. national security, as well as foreign policy and economic interests.[70]

Beijing has only further imposed its national security regime on Hong Kong since then. In March 2024, Hong Kong lawmakers unanimously passed Article 23, known formally as the Safeguarding National Security Ordinance ("SNSO"), which further broadens the scope and definition of political crimes of the 2020 National

---

65 CONG. RESEARCH SERVICE, *Hong Kong Under the National Security Law* (Nov. 15, 2023), https://www.congress.gov/crs-product/R47844.

66 COUNCIL ON FOREIGN RELATIONS, *Assessing China's Digital Silk Road Initiative* (last accessed Sept. 9, 2025), https://www.cfr.org/china-digital-silk-road/.

67 HONG KONG TRADE DEVELOPMENT COUNCIL, *Hong Kong: The Digital Silk Road Super-Hub* (Oct. 19, 2019), https://beltandroad.hktdc.com/en/insights/hong-kong-digital-silk-road-super-hub.

68 CONG. RESEARCH SERVICE, *Hong Kong Under the National Security Law*.

69 CONG. RESEARCH SERVICE, *Hong Kong Adopts New National Security Ordinance: Article 23* (Apr. 1 2024), https://www.congress.gov/crs-product/IN12341.

70 E.O. 13936.

[[FOR PUBLIC INSPECTION; E.O. 13913 CONFIDENTIAL INFORMATION REDACTED]]

Security Law, and targets "external interference" and theft of state secrets, and prohibits foreign political organizations or bodies from conducting political activities in Hong Kong, among other provisions.[71] According to Amnesty International, Article 23 draws its definition of "national security" from mainland China, where it is a vague concept covering "major interests of the state." The ordinance also introduces mainland China's definition of "state secrets," which is extremely broad and can relate to any economic, social, technological or scientific developments, even when they have never been officially classified as secrets. The Chief Executive of Hong Kong has the authority to certify whether any material involves state secrets. Article 23 also creates the new offense of "external interference," which targets collaboration between any person and "external forces." Foreign citizens can also be prosecuted if they commit these "crimes" in Hong Kong. The ordinance also introduces a new offense of "acts endangering national security in relation to computers or electronic systems"—with a potential 20-year prison sentence and extraterritorial effect applying to anyone in the world. However, the ordinance does not define these "acts." This lack of legal clarity and the overbroad definition allow room for abuse. Under the new ordinance, the Chief Executive may also make subsidiary legislation anytime on their own initiative in the name of "safeguarding national security." Finally, in a move designed to target the diaspora and refugees who have moved abroad, the ordinance confers new powers on the government to punish PRC citizens overseas who are accused of—not convicted of—committing national security offenses.[72]

To be sure, under mainland China's cross-border data-transfer requirement, Hong Kong is still technically treated as a foreign jurisdiction. However, should a conflict arise between Hong Kong's own data security law, the Personal Data Privacy Ordinance ("PDPO") and the NSL, the NSL could prevail.[73] This scenario demonstrates the Committee's national security concerns regarding telecommunications connectivity with Hong Kong, as the NSL erodes Hong Kong's autonomy and ability to operate independently of the PRC central government.

In its March 2025 annual report to Congress on the conditions in Hong Kong, the U.S. Department of State reported that throughout 2024, Beijing took new actions which directly threaten U.S. interests and are inconsistent with the Hong

---

71 Lindsay Maizland and Clara Fong; COUNCIL ON FOREIGN RELATIONS, *Backgrounder: Hong Kong's Freedoms: What China Promised and How It's Cracking Down* (last updated July 3, 2025), https://www.cfr.org/backgrounder/hong-kong-freedoms-democracy-protests-china-crackdown.

72 AMNESTY INTERNATIONAL, *What is Hong Kong's Article 23 Law? 10 Things You Need to Know* (Mar. 22, 2024), https://www.amnesty.org/en/latest/news/2024/03/what-is-hong-kongs-article-23-law-10-things-you-need-to-know/.

73 *See* Catherine Leung and Jezamine Fewins, LEWIS SILKIN, *Employers Duties under the National Security Law from a Data Privacy Perspective* (Aug. 16, 2020), https://www.lewissilkin.com/insights/2020/08/17/employers-duties-under-the-national-security-law-from-a-data-privacy-perspective.

[[FOR PUBLIC INSPECTION; E.O. 13913 CONFIDENTIAL INFORMATION REDACTED]]

Kong Basic Law.[74] The State Department assessed that "Beijing permits Hong Kong to retain some differences from mainland China … only so far as these policies offer unique contributions to Beijing's interests," and "[t]he overall trend [] has been one of centralization under Beijing."[75] In particular, "China and Hong Kong authorities [have] continued to use 'national security' as a broad and vague basis to undermine the rule of law and protected rights and freedoms."[76] For example, Hong Kong authorities have used national security legislation to "prosecute people and groups expressing views critical of the government," including "those affiliated with the pro-democracy movement."[77] Beijing and Hong Kong have used national security as a basis to "erod[e] Hong Kong's judicial independence and rule of law," making it so that "there was no expectation of a fair trial" in "cases where authorities asserted a nexus to national security."[78] Reforms to include "national security education" in Hong Kong have "restricted expression" in academic institutions, with a Hong Kong lawmaker stating that "Beijing would closely monitor Hong Kong's implementation of 'patriotic education.'"[79] Overall, the centralization of Hong Kong's policies under Beijing, especially as related to national security, have eroded a wide variety of the rights and freedoms of the people of Hong Kong.[80]

In addition to Beijing's imposition of its national security regime over Hong Kong, the law enforcement and security services of the two jurisdictions appear to be increasing their collaboration, further raising concerns associated with business in Hong Kong. Since the NSL was imposed, the PRC has increasingly exercised police and security power in Hong Kong, including against U.S. citizens who are publicly critical of the PRC. For example, in 2023, the Hong Kong Police Force, pursuant to the NSL, issued international bounties leading to arrests of eight pro-democracy activists who no longer lived in Hong Kong.[81] In November 2024, a

---

74 STATE DEP'T BUREAU OF EAST ASIAN AND PACIFIC AFFAIRS, Report to Congress on Conditions in Hong Kong of Interest to the United States Section 1256 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Mar. 31, 2025) (hereinafter "2025 State Department Report on Hong Kong"), https://www.state.gov/hong-kong-policy-act-report-2025/.

75 *Id.*

76 *Id.*

77 *Id.*

78 *Id.*

79 *Id.*

80 *See id.* (explaining that Beijing's actions threatening Hong Kong's independence in relation to matters outside of commercial and trade policy have negatively impacted democratic institutions and universal suffrage; police and security functions; judicial independence and rule of law; the freedoms of speech, expression, press assembly, association, and movement; education and academic freedom, the freedom of religion or belief; *U.S. citizens* critical of China; and cooperation with U.S. authorities, including critical law enforcement matters).

81 U.S. DEP'T OF STATE, *Press Release: Hong Kong's Extra-Territorial Application of the National Security Law*, Press Release (July 3, 2023), https://2021-2025.state.gov/hong-kongs-extra-territorial-application-of-the-national-security-law/.

[[FOR PUBLIC INSPECTION; E.O. 13913 CONFIDENTIAL INFORMATION REDACTED]]

Hong Kong court sentenced 45 pro-democracy advocates, former lawmakers, and journalists up to 10 years in prison for their involvement in a 2020 unofficial primary election, even though it was "peaceful political activity protected by the Basic Law and recognized in the International Covenant on Civil and Political Rights."[82] Using Hong Kong's "expanded" surveillance powers over those holding views contrary to Chinese interests, Hong Kong authorities issued additional arrest warrants and bounties in December 2024 under the NSL and SNSO, targeting democracy advocates overseas.[83] These actions demonstrated Hong Kong's willingness to apply the NSL and SNSO extraterritorially.

While the PRC has demonstrated an ability to exploit private entities through informal means including coercion, Xie and Digitalsystem have several jurisdictional hooks to PRC and Hong Kong which may mean they could be directly, formally compelled to act by PRC and Hong Kong entities. As stated above, the PRC's 2017 National Intelligence Law provides 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*." 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. **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

Digitalsystem's Hong Kong sister company, **[BEGIN CONFID. INFO] [END CONFID. INFO]**, is directly subject to Hong Kong's jurisdiction and regulatory oversight. **[BEGIN CONFID. INFO] [END CONFID. INFO]**. The PRC government, as discussed above, also has the intent and capability to target U.S. companies, including telecommunications companies, extraterritoriality, for example through illicit cyberattacks. This means Digitalsystem's U.S. operations are still at risk of exploitation, especially because **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

*3. Digitalsystem's planned and potential partnerships with **[BEGIN CONFID. INFO] [END CONFID. INFO]** presents risks that Digitalsystem fails to appreciate.*

Digitalsystem plans to rely on **BEGIN CONFID. INFO] [END CONFID. INFO]**.[84]

Digitalsystem plans to **[BEGIN CONFID. INFO] [END CONFID. INFO]** to support its international telecommunications services, and **[BEGIN CONFID.**

82 2025 State Department Report on Hong Kong.

83 *Id.*

84 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

[[FOR PUBLIC INSPECTION; E.O. 13913 CONFIDENTIAL INFORMATION REDACTED]]

INFO] [END CONFID. INFO].[85] Specifically, Digitalsystem relies on **[BEGIN CONFID. INFO] [END CONFID. INFO]**,[86] and Digitalsystem also stated that **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[87]

Despite public information detailing the increasingly close relationship between the PRC and Hong Kong, **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[88] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[89] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

When the Committee questioned Digitalsystem further about its business in **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[90] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[91] **[BEGIN CONFID. INFO] [END CONFID. INFO]**. Information regarding Digitalsystem's specific service providers follows:

a. [BEGIN CONFID. INFO] [END CONFID. INFO]

Digitalsystem initially described **[BEGIN CONFID. INFO] [END CONFID. INFO]**[92] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[93] Digitalsystem stated that after it receives its international Section 214 authorization, **[BEGIN CONFID. INFO] [END CONFID. INFO]** will provide **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[94] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

[BEGIN CONFID. INFO] [END CONFID. INFO].[95] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

[BEGIN CONFID. INFO] [END CONFID. INFO].[96] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

---

85 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.
86 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.
87 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.
88 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.
89 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.
90 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.
91 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.
92 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.
93 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.
94 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.
95 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.
96 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

[[FOR PUBLIC INSPECTION; E.O. 13913 CONFIDENTIAL INFORMATION REDACTED]]

[BEGIN CONFID. INFO] [END CONFID. INFO].[97] [BEGIN CONFID. INFO] [END CONFID. INFO].[98] [BEGIN CONFID. INFO] [END CONFID. INFO].[99] [BEGIN CONFID. INFO] [END CONFID. INFO].

[BEGIN CONFID. INFO] [END CONFID. INFO].

b. [BEGIN CONFID. INFO] [END CONFID. INFO]

Digitalsystem's current and future potential relationship with [BEGIN CONFID. INFO] [END CONFID. INFO] also presents significant national security concerns. [BEGIN CONFID. INFO] [END CONFID. INFO].[100] [BEGIN CONFID. INFO] [END CONFID. INFO].

[BEGIN CONFID. INFO] [END CONFID. INFO].[101] [BEGIN CONFID. INFO] [END CONFID. INFO]:

- [BEGIN CONFID. INFO] [END CONFID. INFO];[102]
- [BEGIN CONFID. INFO] [END CONFID. INFO];[103]
- [BEGIN CONFID. INFO] [END CONFID. INFO];[104] and
- [BEGIN CONFID. INFO] [END CONFID. INFO].[105]

[BEGIN CONFID. INFO] [END CONFID. INFO].[106] [BEGIN CONFID. INFO] [END CONFID. INFO].[107] [BEGIN CONFID. INFO] [END CONFID. INFO].[108]

Following questioning by the Committee regarding Digitalsystem's current and future plans regarding [BEGIN CONFID. INFO] [END CONFID. INFO], Digitalsystem stated that it [BEGIN CONFID. INFO] [END CONFID. INFO].[109]

---

97 [BEGIN CONFID. INFO] [END CONFID. INFO].

98 [BEGIN CONFID. INFO] [END CONFID. INFO].

99 [BEGIN CONFID. INFO] [END CONFID. INFO].

100 [BEGIN CONFID. INFO] [END CONFID. INFO].

101 [BEGIN CONFID. INFO] [END CONFID. INFO].

102 [BEGIN CONFID. INFO] [END CONFID. INFO].

103 [BEGIN CONFID. INFO] [END CONFID. INFO].

104 [BEGIN CONFID. INFO] [END CONFID. INFO].

105 [BEGIN CONFID. INFO] [END CONFID. INFO].

106 [BEGIN CONFID. INFO] [END CONFID. INFO].

107 [BEGIN CONFID. INFO] [END CONFID. INFO].

108 [BEGIN CONFID. INFO] [END CONFID. INFO].

109 [BEGIN CONFID. INFO] [END CONFID. INFO].

[[FOR PUBLIC INSPECTION; E.O. 13913 CONFIDENTIAL INFORMATION REDACTED]]

[BEGIN CONFID. INFO] [END CONFID. INFO].

Digitalsystem also provided ambiguous answers regarding whether it would provide services **[BEGIN CONFID. INFO] [END CONFID. INFO].**[110] **[BEGIN CONFID. INFO] [END CONFID. INFO].**[111] **[BEGIN CONFID. INFO] [END CONFID. INFO].**[112]

B. Digitalsystem's responses to the Committee raise doubts about its truthfulness and ability to be a trusted compliance partner with the U.S. Government.

Complete, 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. As multiple courts have recognized in upholding the [FCC's] revocation of licenses, "[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."[113]

Throughout this 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. The Committee often rephrased its questions, repeated its questions, or asked series of specific follow-up questions that sometimes resulted in Digitalsystem revealing a different conclusion than it originally stated. Digitalsystem also at no time sought clarification of any question, if it had misunderstood any question. It appears to the Committee that Digitalsystem often provided an initial response that suggested a stronger security position than Digitalsystem was able to support upon follow-up questioning. Digitalsystem provided conflicting and/or misleading responses regarding multiple topics of significance to the Committee's review and assessment.

---

110 **[BEGIN CONFID. INFO] [END CONFID. INFO].**

111 **[BEGIN CONFID. INFO] [END CONFID. INFO].**

112 **[BEGIN CONFID. INFO] [END CONFID. INFO].**

113 *China Unicom (Americas) Operations Ltd.*, 124 F.4th at 1154; *see also China Telecom*, 57 F.4th at 267–68 (upholding revocation of Section 214 authorizations based on "inaccurate, incomplete, or misleading representations to government agencies" about "the potential disruption or misrouting of U.S. communications"); *Pac. Networks Corp. v. FCC*, 77 F.4th 1160, at 1165 (upholding the FCC's revocation of Section 214 authorizations based in part on the licensees' candor, explaining that "national-security risks … plainly heighten any trustworthiness concerns.")

[[FOR PUBLIC INSPECTION; E.O. 13913 CONFIDENTIAL INFORMATION REDACTED]]

*1. Digitalsystem provided conflicting responses regarding **[BEGIN CONFID. INFO] [END CONFID. INFO]**.*

[BEGIN CONFID. INFO] [END CONFID. INFO].[114] However, Digitalsystem's public website **[BEGIN CONFID. INFO] [END CONFID. INFO]** advertises that Digitalsystem has a "strong presence in multiple countries, including Mexico, Brazil, Hong Kong, *and China*."[115] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[116]

[BEGIN CONFID. INFO] [END CONFID. INFO].[117] However, within the same answer, Digitalsystem stated that **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[118] Digitalsystem further explained that **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[119]

*2. Digitalsystem provided conflicting responses regarding partnerships with **[BEGIN CONFID. INFO] [END CONFID. INFO]**.*

Digitalsystem provided inconsistent responses regarding additional **[BEGIN CONFID. INFO] [END CONFID. INFO]** companies with which it might work, raising the possibility that it would work with such companies if permitted to do so. Digitalsystem initially stated that it **[BEGIN CONFID. INFO] [END CONFID. INFO],**[120] **[BEGIN CONFID. INFO] [END CONFID. INFO]**. However, as stated above, it separately identified **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

However, at the time it provided responses, Digitalsystem's website publicly listed many companies based in, or affiliated with, the PRC and Russia as "Partners" for different services (though many of these services are not telecommunications services, and it is not clear whether these were all services within the United States or provided by Digitalsystem's international affiliates). For example, Digitalsystem's website listed as "Partners:" China Mobile, China Telecom, Dahua, Fanvil (PRC company), Hikvision, Huawei, Yealink, ZTE, Zyxel, and Rostelecom (Russia), in addition to China Unicom and PCCW.[121] Following

---

114 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

115 *About Us*, DIGITALSYSTEM, https://www.digitalsystem.net/about-us.html (emphasis added).

116 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

117 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

118 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

119 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

120 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

121 **[BEGIN CONFID. INFO] [END CONFID. INFO]**. DOJ's National Security Division, Foreign Investment Review Section has screenshots of the relevant pages upon request on file, however all or most of the companies appear to be listed as of February 9, 2025, though now under a banner reading "Clients who trust us." Equipment and/or services provided by the U.S. affiliates/subsidiaries of Huawei, ZTE, Hikvision, Dahua, China Mobile, China Telecom, and China Unicom appear on the FCC's Covered List. *See* FCC, *List of Equipment and Services Covered by*

[[FOR PUBLIC INSPECTION; E.O. 13913 CONFIDENTIAL INFORMATION REDACTED]]

questioning, Digitalsystem largely stated that **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[122] Digitalsystem further stated that:

[BEGIN CONFID. INFO] [END CONFID. INFO].[123]

[BEGIN CONFID. INFO] [END CONFID. INFO].[124]

[BEGIN CONFID. INFO] [END CONFID. INFO].

a. [BEGIN CONFID. INFO] [END CONFID. INFO]

[BEGIN CONFID. INFO] [END CONFID. INFO].[125] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

[BEGIN CONFID. INFO] [END CONFID. INFO].[126] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[127]

b. [BEGIN CONFID. INFO] [END CONFID. INFO]

Digitalsystem's responses regarding future business with **[BEGIN CONFID. INFO] [END CONFID. INFO]** were inconsistent. Though it originally raised that it would **[BEGIN CONFID. INFO] [END CONFID. INFO]**, following questioning it eventually said that Digitalsystem has "**[BEGIN CONFID. INFO] [END CONFID. INFO]**"[128] and "**[BEGIN CONFID. INFO] [END CONFID. INFO]**."[129]

[BEGIN CONFID. INFO] [END CONFID. INFO].[130] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[131]

Further highlighting the conflicting responses described above, since Digitalsystem provided the responses, it updated its website to remove the phrase "Partners," instead listing the relevant companies under a banner reading "Clients

---

Section 2 of The Secure Networks Act (last visited Sept. 8, 2025), fcc.gov/supplychain/coveredlist.

122 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

123 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

124 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

125 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

126 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

127 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

128 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

129 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

130 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

131 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

[[FOR PUBLIC INSPECTION; E.O. 13913 CONFIDENTIAL INFORMATION REDACTED]]

who trust us."[132] This website description now implies that the listed companies are customers of Digitalsystem, **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

In sum, third parties—especially those based in Hong Kong and the PRC—have significant intent and capability to harm U.S. national security and law enforcement interests through U.S. telecommunications companies. As explained, such companies are subject to the jurisdiction, direction, and control of the PRC and Hong Kong governments, especially given these jurisdictions' ever-expanding national security laws. Coupled with Digitalsystem's inconsistent and ambiguous responses regarding **[BEGIN CONFID. INFO] [END CONFID. INFO]**, the Committee has significant concerns with these relationships and Digitalsystem's ability to adequately mitigate risk stemming from these potential partnerships.

3. Digitalsystem provided misleading responses regarding the extent of its owners' access to company records and systems.

Digitalsystem's responses originally described **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[133] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[134] Digitalsystem further stated **[BEGIN CONFID. INFO] [END CONFID. INFO]**,[135] it later stated **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[136] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

[BEGIN CONFID. INFO] [END CONFID. INFO].[137] **[BEGIN CONFID. INFO] [END CONFID. INFO]**[138] **[BEGIN CONFID. INFO] [END CONFID. INFO]**[139]).

[BEGIN CONFID. INFO] [END CONFID. INFO].[140] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

[BEGIN CONFID. INFO] [END CONFID. INFO].[141] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[142] **[BEGIN CONFID. INFO] [END CONFID.**

---

132 *Services*, DIGITALSYSTEM, https://www.digitalsystem.net/services/network.html (last visited Feb. 9, 2026).

133 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

134 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

135 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

136 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

137 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

138 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

139 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

140 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

141 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

142 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

[[FOR PUBLIC INSPECTION; E.O. 13913 CONFIDENTIAL INFORMATION REDACTED]]

INFO].

4. Digitalsystem provided conflicting responses regarding the number and location of foreign individuals with access to Digitalsystem's U.S. records, data, and equipment.

Digitalsystem initially stated **[BEGIN CONFID. INFO] [END CONFID. INFO]**. However, Digitalsystem later revealed that **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

Digitalsystem initially stated that it **[BEGIN CONFID. INFO] [END CONFID. INFO]**[143] but it actually appears **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[144] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[145] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[146] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[147] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[148]

Despite 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. This impeded the Committee's ability to fully assess the risks associated with such access and consider appropriate mitigation measures to address those risks.

Digitalsystem stated that **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[149] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[150] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[151]

5. Digitalsystem provided conflicting responses regarding its lawful U.S. process and lawful intercept capabilities.

Digitalsystem initially stated that **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[152] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[153]

---

143 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

144 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

145 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

146 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

147 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

148 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

149 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

150 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

151 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

152 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

153 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

[[FOR PUBLIC INSPECTION; E.O. 13913 CONFIDENTIAL INFORMATION REDACTED]]

However, when the Committee asked Digitalsystem **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[154] **[BEGIN CONFID. INFO] [END CONFID. INFO]**,[155] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[156] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

[BEGIN CONFID. INFO] [END CONFID. INFO].

C. There are significant vulnerabilities associated with Digitalsystem's planned business that cannot be adequately mitigated.

Digitalsystem is seeking an international Section 214 authorization to provide both facilities-based and resold services, meaning that it would directly handle communications and access U.S. customer records and communications-related data, including PII, Call Detail Records ("CDRs"), billing records, and more. **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

1. *Certain U.S. data will be stored and accessed [BEGIN CONFID. INFO] [END CONFID. INFO].*

Digitalsystem stores its full U.S. records and data **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[157] Digitalsystem indicated that it also stores **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[158]

[BEGIN CONFID. INFO] [END CONFID. INFO].[159] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

2. *Digitalsystem plans to [BEGIN CONFID. INFO] [END CONFID. INFO].*

[BEGIN CONFID. INFO] [END CONFID. INFO].[160] **[BEGIN CONFID. INFO] [END CONFID. INFO]**.[161]

[BEGIN CONFID. INFO] [END CONFID. INFO].

---

154 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.
155 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.
156 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.
157 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.
158 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.
159 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.
160 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.
161 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

[[FOR PUBLIC INSPECTION; E.O. 13913 CONFIDENTIAL INFORMATION REDACTED]]

3. [BEGIN CONFID. INFO] [END CONFID. INFO].

[BEGIN CONFID. INFO] [END CONFID. INFO].[162] **[BEGIN CONFID. INFO] [END CONFID. INFO].**[163] **[BEGIN CONFID. INFO] [END CONFID. INFO].**[164]

[BEGIN CONFID. INFO] [END CONFID. INFO].

[BEGIN CONFID. INFO] [END CONFID. INFO].

[BEGIN CONFID. INFO] [END CONFID. INFO].

These vulnerabilities are likely to increase if Digitalsystem gains a Section 214 authorization and begins offering facilities-based communication services, which will increase the amount and sensitivity of the communications-related data for which Digitalsystem is responsible.

D. If the FCC granted Digitalsystem a Section 214 authorization and threat actors exploited the vulnerabilities associated with the business, there would be significant negative consequences for U.S. national security and law enforcement interests.

Digitalsystem currently has **[BEGIN CONFID. INFO] [END CONFID. INFO]** customer base for telecommunications services, but this customer base would likely expand once Digitalsystem receives an international Section 214 authorization. **[BEGIN CONFID. INFO] [END CONFID. INFO]**. Once granted the international Section 214 authorization, Digitalsystem intends to expand its telecommunications service offerings and customer base, focusing generally on **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

While the impact associated with **[BEGIN CONFID. INFO] [END CONFID. INFO]**, the impact would increase as Digitalsystem gains an international Section 214 authorization and starts serving **[BEGIN CONFID. INFO] [END CONFID. INFO]** telecommunications customers. If Digitalsystem, Xie, or third-party threat actors were to exploit the vulnerabilities described in this analysis, there are several consequences that could occur:

1. Threat actors could collect or exfiltrate U.S. communications content and sensitive U.S. records.

If 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. The types of information collected by a

162 **[BEGIN CONFID. INFO] [END CONFID. INFO].**

163 **[BEGIN CONFID. INFO] [END CONFID. INFO].**

164 **[BEGIN CONFID. INFO] [END CONFID. INFO].**

[[FOR PUBLIC INSPECTION; E.O. 13913 CONFIDENTIAL INFORMATION REDACTED]]

facilities-based telecommunications provider are especially sensitive, typically including not only customer identifying information and bank account and billing information, but CDRs, Internet Protocol Detail Records ("IPDRs"), and the contents of communications themselves (such as text messages, voicemails, and call records). Such information could be used, for example 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). In the aggregate, the information could also enable bulk collection and analysis of information on U.S. persons.

2. Threat actors could disrupt U.S. communications.

As 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. A threat actor could target Digitalsystem's networks and equipment in the United States—**[BEGIN CONFID. INFO] [END CONFID. INFO]**—and access or prevent the equipment from working properly. Given that Digitalsystem plans to generally serve **[BEGIN CONFID. INFO] [END CONFID. INFO]**, but depending on the type and extent of Digitalsystem's future customer base, could affect certain populations and industries.

3. Threat actors could facilitate the misrouting of U.S. communications to jurisdictions of concern.

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 **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

If 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 **[BEGIN CONFID. INFO] [END CONFID. INFO]**) wished to do so and could gain control over Digitalsystem's management network, these parties could direct traffic intended for the United States or other locations through Hong Kong or mainland China. 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 resource to protect sensitive data, would likely allow for collection of this data.

4. Threat actors could expose lawful U.S. process to foreign adversaries.

As a facilities-based provider, Digitalsystem would be directly responsible for effectuating lawful U.S. process requests, including supporting the installation of wiretaps or collecting other types of communications, and producing U.S. customer records for law enforcement. **[BEGIN CONFID. INFO] [END CONFID. INFO]**.

[[FOR PUBLIC INSPECTION; E.O. 13913 CONFIDENTIAL INFORMATION REDACTED]]

Though Digitalsystem states that **[BEGIN CONFID. INFO] [END CONFID. INFO]**, the vulnerabilities described above raise doubts about Digitalsystem's ability to protect lawful U.S. process. If these vulnerabilities were exploited by threat actors including PRC intelligence services, there could be significant consequences for U.S. law enforcement and national security equities. Exploitation 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.

VI. Conclusion

This application presents immitigable and unacceptable risks to U.S. national security and law enforcement interests and should be denied. If the FCC granted Digitalsystem authority pursuant to Section 214 to provide international telecommunications, there is a significant risk that those 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. Digitalsystem's plans for its Section 214 authorization—which include services **[BEGIN CONFID. INFO] [END CONFID. INFO]**, partnership **[BEGIN CONFID. INFO] [END CONFID. INFO]** with **[BEGIN CONFID. INFO] [END CONFID. INFO]**, and relationships and potential relationships with **[BEGIN CONFID. INFO] [END CONFID. INFO]** service providers—exacerbate those risks. Given Digitalsystem's inconsistent and changed responses throughout the review, which raise doubts as to its candor, as well as its position that **[BEGIN CONFID. INFO] [END CONFID. INFO]**, Digitalsystem is not a reliable partner to carry out mitigation measures of any type, nor do such measures appear feasible given Digitalsystem's business plans. Accordingly, the Committee recommends that the FCC deny the Applicant's application for authority pursuant to Section 214.

[[FOR PUBLIC INSPECTION; E.O. 13913 CONFIDENTIAL INFORMATION REDACTED]]

Respectfully submitted:

David Brodian
Chief Counsel, National Telecommunications and Information Administration
U.S. Department of Commerce, Rm. 4713
1401 Constitution Ave., N.W.
Washington, D.C. 20230
(202) 482-1816

On behalf of the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector