FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 30, 2023

The Honorable Ron Wyden
United States Senate
221 Dirksen Senate Office Building
Washington, DC 20510

Dear Senator Wyden:

Thank you for your letter regarding the risks foreign-managed service providers may pose to telecommunications networks in the United States. I agree with you that the surveillance threats to communications infrastructure in this country are not limited to the presence of insecure, foreign-manufactured technology in our networks. That is why I have had the Federal Communications Commission take a "whole of network" approach to improving the security of our communications networks. As part of this effort, I look forward to working with you to ensure that the United States appropriately assesses the risks posed from service providers outsourcing the administration of their networks to foreign entities.

At the Commission, I have made network security a top priority. To start, the agency has taken significant steps to improve awareness of network vulnerabilities and threats involving both the public and private sector. On March 12, 2021, the Commission published the first-ever list of communications and services that pose an unacceptable risk to national security, consistent with the Secure and Trusted Communications Networks Act. This initial list, known as the Covered List, included equipment from Chinese companies Huawei, ZTE, Hytera, Hikvision, and Dahua. Since then, we have added to the Covered List equipment and services from five additional entities: China Mobile, China Telecom, China Unicom, Pacific Networks and its wholly owned subsidiary ComNet, and Kaspersky Lab. The agency's rules prohibit the use of Universal Service funds to purchase or obtain any equipment or services on the Covered List. In addition, this list provides clear notice to private companies making purchasing decisions that the Commission has concluded that these entities produce equipment and services that pose an unacceptable risk to our national security. Other steps we have taken to improve awareness of network vulnerabilities include a proposal I have shared with my colleagues to implement stricter data breach reporting and work with the Department of State to update our coordination practices regarding national security issues related to submarine cable licenses.

The Commission also has taken concrete action to defend against the threats and vulnerabilities that have been identified through this work and the efforts of our national security colleagues. For the first time, the agency adopted rules to prohibit the authorization of telecommunications and video surveillance equipment for national security reasons. We launched the Secure and Trusted Communications Networks Reimbursement Program to remove untrusted equipment from our networks and replace them with secure alternatives. Working with our national security colleagues, we revoked the section 214 operating authorities of four Chinese state-owned carriers who were providing service in the United States. We started a

rulemaking to require Emergency Alert System and Wireless Emergency Alert System participants to have a cybersecurity risk management plan in place and to install the most recent security patches. Recognizing that the equipment that connects to our networks is just as consequential for security as the equipment that goes into our networks, the agency also launched a new inquiry on the security of the internet of things.

Finally, the Commission has taken steps to build security into what comes next. I have revitalized the Cybersecurity Forum for Independent and Executive Branch Regulators to enhance the security of critical infrastructure. The Forum brings together the leadership of 32 federal agencies with regulatory oversight of critical sectors, including independent agencies such as the Securities and Exchange Commission, the Commodities Futures Trading Commission, the Consumer Product Safety Commission, the Federal Energy Regulatory Commission, and the Nuclear Regulatory Commission, and executive branch regulatory agencies, such as the Environmental Protection Agency, the Department of Health and Human Services, the Department of Transportation, and the Department of Homeland Security, as well as others, to coordinate efforts. Through this group, agencies with different authorities and different missions and responsibilities are working together to identify and leverage opportunities to harmonize federal oversight to reduce cyber risk while not imposing undue burdens on owners and operators of critical infrastructure. I also rechartered the Communications Security, Reliability, and Interoperability Council and, for the first time, designated the Cybersecurity and Infrastructure Security Agency as co-chair. I gave this new council a 5G focus and asked it to review risks to service provider operations from attacks in software and cloud service stacks and to develop mitigation strategies. On top of this, we are promoting cybersecurity innovation through our inquiry on open radio access networks and two new innovation zones for advanced wireless communications and network innovation research.

Of course, as you recognize, national security risks are constantly evolving, and this requires new focus on whether foreign firms that provide services to telecommunications providers in the United States pose a threat to our national security. To this end, I have had the agency reach out to our national security colleagues, including CISA and the Office of the Director of National Intelligence, to coordinate on this issue. Last year, CISA joined with partners from the United Kingdom, Australia, Canada, and New Zealand to issue a joint cybersecurity advisory to provide guidance on how to protect against malicious cyber activity targeting managed service providers and their customers. This cybersecurity advisory follows a set of risk considerations issued in 2021 by CISA's National Risk Management Center, as well as CISA's guidance for small- and mid-sized businesses using managed service providers to manage IT systems, store data, or support sensitive processes. I am continuing to assess this issue with CISA and our other partners, including through the Cybersecurity Forum for Independent and Executive Branch Regulators noted above, and we are seeking to understand the extent to which agencies have developed a record on the risks posed by foreign management of United States networks. In addition, in January I announced that I intend to share with my colleagues a proposed rulemaking that would provide a framework for national security agencies to reassess a foreign carrier's authorization to provide service in the United States on an ongoing basis. As part of that rulemaking, we will also seek comment on the issues you have raised regarding the foreign management of United States telecommunications networks.

I appreciate your interest in national security and the need to evolve our policies regarding telecommunications. I would be happy to keep your office updated as we continue to work on these matters and collaborate with our national security colleagues.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 30, 2023

The Honorable Chris Van Hollen
United States Senate
110 Hart Senate Office Building
Washington, DC 20510

Dear Senator Van Hollen:

Thank you for your letter regarding the risks foreign-managed service providers may pose to telecommunications networks in the United States. I agree with you that the surveillance threats to communications infrastructure in this country are not limited to the presence of insecure, foreign-manufactured technology in our networks. That is why I have had the Federal Communications Commission take a "whole of network" approach to improving the security of our communications networks. As part of this effort, I look forward to working with you to ensure that the United States appropriately assesses the risks posed from service providers outsourcing the administration of their networks to foreign entities.

At the Commission, I have made network security a top priority. To start, the agency has taken significant steps to improve awareness of network vulnerabilities and threats involving both the public and private sector. On March 12, 2021, the Commission published the first-ever list of communications and services that pose an unacceptable risk to national security, consistent with the Secure and Trusted Communications Networks Act. This initial list, known as the Covered List, included equipment from Chinese companies Huawei, ZTE, Hytera, Hikvision, and Dahua. Since then, we have added to the Covered List equipment and services from five additional entities: China Mobile, China Telecom, China Unicom, Pacific Networks and its wholly owned subsidiary ComNet, and Kaspersky Lab. The agency's rules prohibit the use of Universal Service funds to purchase or obtain any equipment or services on the Covered List. In addition, this list provides clear notice to private companies making purchasing decisions that the Commission has concluded that these entities produce equipment and services that pose an unacceptable risk to our national security. Other steps we have taken to improve awareness of network vulnerabilities include a proposal I have shared with my colleagues to implement stricter data breach reporting and work with the Department of State to update our coordination practices regarding national security issues related to submarine cable licenses.

The Commission also has taken concrete action to defend against the threats and vulnerabilities that have been identified through this work and the efforts of our national security colleagues. For the first time, the agency adopted rules to prohibit the authorization of telecommunications and video surveillance equipment for national security reasons. We launched the Secure and Trusted Communications Networks Reimbursement Program to remove untrusted equipment from our networks and replace them with secure alternatives. Working with our national security colleagues, we revoked the section 214 operating authorities of four Chinese state-owned carriers who were providing service in the United States. We started a

rulemaking to require Emergency Alert System and Wireless Emergency Alert System participants to have a cybersecurity risk management plan in place and to install the most recent security patches. Recognizing that the equipment that connects to our networks is just as consequential for security as the equipment that goes into our networks, the agency also launched a new inquiry on the security of the internet of things.

Finally, the Commission has taken steps to build security into what comes next. I have revitalized the Cybersecurity Forum for Independent and Executive Branch Regulators to enhance the security of critical infrastructure. The Forum brings together the leadership of 32 federal agencies with regulatory oversight of critical sectors, including independent agencies such as the Securities and Exchange Commission, the Commodities Futures Trading Commission, the Consumer Product Safety Commission, the Federal Energy Regulatory Commission, and the Nuclear Regulatory Commission, and executive branch regulatory agencies, such as the Environmental Protection Agency, the Department of Health and Human Services, the Department of Transportation, and the Department of Homeland Security, as well as others, to coordinate efforts. Through this group, agencies with different authorities and different missions and responsibilities are working together to identify and leverage opportunities to harmonize federal oversight to reduce cyber risk while not imposing undue burdens on owners and operators of critical infrastructure. I also rechartered the Communications Security, Reliability, and Interoperability Council and, for the first time, designated the Cybersecurity and Infrastructure Security Agency as co-chair. I gave this new council a 5G focus and asked it to review risks to service provider operations from attacks in software and cloud service stacks and to develop mitigation strategies. On top of this, we are promoting cybersecurity innovation through our inquiry on open radio access networks and two new innovation zones for advanced wireless communications and network innovation research.

Of course, as you recognize, national security risks are constantly evolving, and this requires new focus on whether foreign firms that provide services to telecommunications providers in the United States pose a threat to our national security. To this end, I have had the agency reach out to our national security colleagues, including CISA and the Office of the Director of National Intelligence, to coordinate on this issue. Last year, CISA joined with partners from the United Kingdom, Australia, Canada, and New Zealand to issue a joint cybersecurity advisory to provide guidance on how to protect against malicious cyber activity targeting managed service providers and their customers. This cybersecurity advisory follows a set of risk considerations issued in 2021 by CISA's National Risk Management Center, as well as CISA's guidance for small- and mid-sized businesses using managed service providers to manage IT systems, store data, or support sensitive processes. I am continuing to assess this issue with CISA and our other partners, including through the Cybersecurity Forum for Independent and Executive Branch Regulators noted above, and we are seeking to understand the extent to which agencies have developed a record on the risks posed by foreign management of United States networks. In addition, in January I announced that I intend to share with my colleagues a proposed rulemaking that would provide a framework for national security agencies to reassess a foreign carrier's authorization to provide service in the United States on an ongoing basis. As part of that rulemaking, we will also seek comment on the issues you have raised regarding the foreign management of United States telecommunications networks.

I appreciate your interest in national security and the need to evolve our policies regarding telecommunications. I would be happy to keep your office updated as we continue to work on these matters and collaborate with our national security colleagues.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 30, 2023

The Honorable Richard Blumenthal
United States Senate
706 Hart Senate Office Building
Washington, DC 20510

Dear Senator Blumenthal:

Thank you for your letter regarding the risks foreign-managed service providers may pose to telecommunications networks in the United States. I agree with you that the surveillance threats to communications infrastructure in this country are not limited to the presence of insecure, foreign-manufactured technology in our networks. That is why I have had the Federal Communications Commission take a "whole of network" approach to improving the security of our communications networks. As part of this effort, I look forward to working with you to ensure that the United States appropriately assesses the risks posed from service providers outsourcing the administration of their networks to foreign entities.

At the Commission, I have made network security a top priority. To start, the agency has taken significant steps to improve awareness of network vulnerabilities and threats involving both the public and private sector. On March 12, 2021, the Commission published the first-ever list of communications and services that pose an unacceptable risk to national security, consistent with the Secure and Trusted Communications Networks Act. This initial list, known as the Covered List, included equipment from Chinese companies Huawei, ZTE, Hytera, Hikvision, and Dahua. Since then, we have added to the Covered List equipment and services from five additional entities: China Mobile, China Telecom, China Unicom, Pacific Networks and its wholly owned subsidiary ComNet, and Kaspersky Lab. The agency's rules prohibit the use of Universal Service funds to purchase or obtain any equipment or services on the Covered List. In addition, this list provides clear notice to private companies making purchasing decisions that the Commission has concluded that these entities produce equipment and services that pose an unacceptable risk to our national security. Other steps we have taken to improve awareness of network vulnerabilities include a proposal I have shared with my colleagues to implement stricter data breach reporting and work with the Department of State to update our coordination practices regarding national security issues related to submarine cable licenses.

The Commission also has taken concrete action to defend against the threats and vulnerabilities that have been identified through this work and the efforts of our national security colleagues. For the first time, the agency adopted rules to prohibit the authorization of telecommunications and video surveillance equipment for national security reasons. We launched the Secure and Trusted Communications Networks Reimbursement Program to remove untrusted equipment from our networks and replace them with secure alternatives. Working with our national security colleagues, we revoked the section 214 operating authorities of four Chinese state-owned carriers who were providing service in the United States. We started a

rulemaking to require Emergency Alert System and Wireless Emergency Alert System participants to have a cybersecurity risk management plan in place and to install the most recent security patches. Recognizing that the equipment that connects to our networks is just as consequential for security as the equipment that goes into our networks, the agency also launched a new inquiry on the security of the internet of things.

Finally, the Commission has taken steps to build security into what comes next. I have revitalized the Cybersecurity Forum for Independent and Executive Branch Regulators to enhance the security of critical infrastructure. The Forum brings together the leadership of 32 federal agencies with regulatory oversight of critical sectors, including independent agencies such as the Securities and Exchange Commission, the Commodities Futures Trading Commission, the Consumer Product Safety Commission, the Federal Energy Regulatory Commission, and the Nuclear Regulatory Commission, and executive branch regulatory agencies, such as the Environmental Protection Agency, the Department of Health and Human Services, the Department of Transportation, and the Department of Homeland Security, as well as others, to coordinate efforts. Through this group, agencies with different authorities and different missions and responsibilities are working together to identify and leverage opportunities to harmonize federal oversight to reduce cyber risk while not imposing undue burdens on owners and operators of critical infrastructure. I also rechartered the Communications Security, Reliability, and Interoperability Council and, for the first time, designated the Cybersecurity and Infrastructure Security Agency as co-chair. I gave this new council a 5G focus and asked it to review risks to service provider operations from attacks in software and cloud service stacks and to develop mitigation strategies. On top of this, we are promoting cybersecurity innovation through our inquiry on open radio access networks and two new innovation zones for advanced wireless communications and network innovation research.

Of course, as you recognize, national security risks are constantly evolving, and this requires new focus on whether foreign firms that provide services to telecommunications providers in the United States pose a threat to our national security. To this end, I have had the agency reach out to our national security colleagues, including CISA and the Office of the Director of National Intelligence, to coordinate on this issue. Last year, CISA joined with partners from the United Kingdom, Australia, Canada, and New Zealand to issue a joint cybersecurity advisory to provide guidance on how to protect against malicious cyber activity targeting managed service providers and their customers. This cybersecurity advisory follows a set of risk considerations issued in 2021 by CISA's National Risk Management Center, as well as CISA's guidance for small- and mid-sized businesses using managed service providers to manage IT systems, store data, or support sensitive processes. I am continuing to assess this issue with CISA and our other partners, including through the Cybersecurity Forum for Independent and Executive Branch Regulators noted above, and we are seeking to understand the extent to which agencies have developed a record on the risks posed by foreign management of United States networks. In addition, in January I announced that I intend to share with my colleagues a proposed rulemaking that would provide a framework for national security agencies to reassess a foreign carrier's authorization to provide service in the United States on an ongoing basis. As part of that rulemaking, we will also seek comment on the issues you have raised regarding the foreign management of United States telecommunications networks.

I appreciate your interest in national security and the need to evolve our policies regarding telecommunications. I would be happy to keep your office updated as we continue to work on these matters and collaborate with our national security colleagues.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 30, 2023

The Honorable Richard J. Durbin
United States Senate
711 Hart Senate Office Building
Washington, DC 20510

Dear Senator Durbin:

Thank you for your letter regarding the risks foreign-managed service providers may pose to telecommunications networks in the United States. I agree with you that the surveillance threats to communications infrastructure in this country are not limited to the presence of insecure, foreign-manufactured technology in our networks. That is why I have had the Federal Communications Commission take a "whole of network" approach to improving the security of our communications networks. As part of this effort, I look forward to working with you to ensure that the United States appropriately assesses the risks posed from service providers outsourcing the administration of their networks to foreign entities.

At the Commission, I have made network security a top priority. To start, the agency has taken significant steps to improve awareness of network vulnerabilities and threats involving both the public and private sector. On March 12, 2021, the Commission published the first-ever list of communications and services that pose an unacceptable risk to national security, consistent with the Secure and Trusted Communications Networks Act. This initial list, known as the Covered List, included equipment from Chinese companies Huawei, ZTE, Hytera, Hikvision, and Dahua. Since then, we have added to the Covered List equipment and services from five additional entities: China Mobile, China Telecom, China Unicom, Pacific Networks and its wholly owned subsidiary ComNet, and Kaspersky Lab. The agency's rules prohibit the use of Universal Service funds to purchase or obtain any equipment or services on the Covered List. In addition, this list provides clear notice to private companies making purchasing decisions that the Commission has concluded that these entities produce equipment and services that pose an unacceptable risk to our national security. Other steps we have taken to improve awareness of network vulnerabilities include a proposal I have shared with my colleagues to implement stricter data breach reporting and work with the Department of State to update our coordination practices regarding national security issues related to submarine cable licenses.

The Commission also has taken concrete action to defend against the threats and vulnerabilities that have been identified through this work and the efforts of our national security colleagues. For the first time, the agency adopted rules to prohibit the authorization of telecommunications and video surveillance equipment for national security reasons. We launched the Secure and Trusted Communications Networks Reimbursement Program to remove untrusted equipment from our networks and replace them with secure alternatives. Working with our national security colleagues, we revoked the section 214 operating authorities of four Chinese state-owned carriers who were providing service in the United States. We started a

rulemaking to require Emergency Alert System and Wireless Emergency Alert System participants to have a cybersecurity risk management plan in place and to install the most recent security patches. Recognizing that the equipment that connects to our networks is just as consequential for security as the equipment that goes into our networks, the agency also launched a new inquiry on the security of the internet of things.

Finally, the Commission has taken steps to build security into what comes next. I have revitalized the Cybersecurity Forum for Independent and Executive Branch Regulators to enhance the security of critical infrastructure. The Forum brings together the leadership of 32 federal agencies with regulatory oversight of critical sectors, including independent agencies such as the Securities and Exchange Commission, the Commodities Futures Trading Commission, the Consumer Product Safety Commission, the Federal Energy Regulatory Commission, and the Nuclear Regulatory Commission, and executive branch regulatory agencies, such as the Environmental Protection Agency, the Department of Health and Human Services, the Department of Transportation, and the Department of Homeland Security, as well as others, to coordinate efforts. Through this group, agencies with different authorities and different missions and responsibilities are working together to identify and leverage opportunities to harmonize federal oversight to reduce cyber risk while not imposing undue burdens on owners and operators of critical infrastructure. I also rechartered the Communications Security, Reliability, and Interoperability Council and, for the first time, designated the Cybersecurity and Infrastructure Security Agency as co-chair. I gave this new council a 5G focus and asked it to review risks to service provider operations from attacks in software and cloud service stacks and to develop mitigation strategies. On top of this, we are promoting cybersecurity innovation through our inquiry on open radio access networks and two new innovation zones for advanced wireless communications and network innovation research.

Of course, as you recognize, national security risks are constantly evolving, and this requires new focus on whether foreign firms that provide services to telecommunications providers in the United States pose a threat to our national security. To this end, I have had the agency reach out to our national security colleagues, including CISA and the Office of the Director of National Intelligence, to coordinate on this issue. Last year, CISA joined with partners from the United Kingdom, Australia, Canada, and New Zealand to issue a joint cybersecurity advisory to provide guidance on how to protect against malicious cyber activity targeting managed service providers and their customers. This cybersecurity advisory follows a set of risk considerations issued in 2021 by CISA's National Risk Management Center, as well as CISA's guidance for small- and mid-sized businesses using managed service providers to manage IT systems, store data, or support sensitive processes. I am continuing to assess this issue with CISA and our other partners, including through the Cybersecurity Forum for Independent and Executive Branch Regulators noted above, and we are seeking to understand the extent to which agencies have developed a record on the risks posed by foreign management of United States networks. In addition, in January I announced that I intend to share with my colleagues a proposed rulemaking that would provide a framework for national security agencies to reassess a foreign carrier's authorization to provide service in the United States on an ongoing basis. As part of that rulemaking, we will also seek comment on the issues you have raised regarding the foreign management of United States telecommunications networks.

I appreciate your interest in national security and the need to evolve our policies regarding telecommunications. I would be happy to keep your office updated as we continue to work on these matters and collaborate with our national security colleagues.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 30, 2023

The Honorable Edward J. Markey
United States Senate
255 Dirksen Senate Office Building
Washington, DC 20510

Dear Senator Markey:

Thank you for your letter regarding the risks foreign-managed service providers may pose to telecommunications networks in the United States. I agree with you that the surveillance threats to communications infrastructure in this country are not limited to the presence of insecure, foreign-manufactured technology in our networks. That is why I have had the Federal Communications Commission take a "whole of network" approach to improving the security of our communications networks. As part of this effort, I look forward to working with you to ensure that the United States appropriately assesses the risks posed from service providers outsourcing the administration of their networks to foreign entities.

At the Commission, I have made network security a top priority. To start, the agency has taken significant steps to improve awareness of network vulnerabilities and threats involving both the public and private sector. On March 12, 2021, the Commission published the first-ever list of communications and services that pose an unacceptable risk to national security, consistent with the Secure and Trusted Communications Networks Act. This initial list, known as the Covered List, included equipment from Chinese companies Huawei, ZTE, Hytera, Hikvision, and Dahua. Since then, we have added to the Covered List equipment and services from five additional entities: China Mobile, China Telecom, China Unicom, Pacific Networks and its wholly owned subsidiary ComNet, and Kaspersky Lab. The agency's rules prohibit the use of Universal Service funds to purchase or obtain any equipment or services on the Covered List. In addition, this list provides clear notice to private companies making purchasing decisions that the Commission has concluded that these entities produce equipment and services that pose an unacceptable risk to our national security. Other steps we have taken to improve awareness of network vulnerabilities include a proposal I have shared with my colleagues to implement stricter data breach reporting and work with the Department of State to update our coordination practices regarding national security issues related to submarine cable licenses.

The Commission also has taken concrete action to defend against the threats and vulnerabilities that have been identified through this work and the efforts of our national security colleagues. For the first time, the agency adopted rules to prohibit the authorization of telecommunications and video surveillance equipment for national security reasons. We launched the Secure and Trusted Communications Networks Reimbursement Program to remove untrusted equipment from our networks and replace them with secure alternatives. Working with our national security colleagues, we revoked the section 214 operating authorities of four Chinese state-owned carriers who were providing service in the United States. We started a

rulemaking to require Emergency Alert System and Wireless Emergency Alert System participants to have a cybersecurity risk management plan in place and to install the most recent security patches. Recognizing that the equipment that connects to our networks is just as consequential for security as the equipment that goes into our networks, the agency also launched a new inquiry on the security of the internet of things.

Finally, the Commission has taken steps to build security into what comes next. I have revitalized the Cybersecurity Forum for Independent and Executive Branch Regulators to enhance the security of critical infrastructure. The Forum brings together the leadership of 32 federal agencies with regulatory oversight of critical sectors, including independent agencies such as the Securities and Exchange Commission, the Commodities Futures Trading Commission, the Consumer Product Safety Commission, the Federal Energy Regulatory Commission, and the Nuclear Regulatory Commission, and executive branch regulatory agencies, such as the Environmental Protection Agency, the Department of Health and Human Services, the Department of Transportation, and the Department of Homeland Security, as well as others, to coordinate efforts. Through this group, agencies with different authorities and different missions and responsibilities are working together to identify and leverage opportunities to harmonize federal oversight to reduce cyber risk while not imposing undue burdens on owners and operators of critical infrastructure. I also rechartered the Communications Security, Reliability, and Interoperability Council and, for the first time, designated the Cybersecurity and Infrastructure Security Agency as co-chair. I gave this new council a 5G focus and asked it to review risks to service provider operations from attacks in software and cloud service stacks and to develop mitigation strategies. On top of this, we are promoting cybersecurity innovation through our inquiry on open radio access networks and two new innovation zones for advanced wireless communications and network innovation research.

Of course, as you recognize, national security risks are constantly evolving, and this requires new focus on whether foreign firms that provide services to telecommunications providers in the United States pose a threat to our national security. To this end, I have had the agency reach out to our national security colleagues, including CISA and the Office of the Director of National Intelligence, to coordinate on this issue. Last year, CISA joined with partners from the United Kingdom, Australia, Canada, and New Zealand to issue a joint cybersecurity advisory to provide guidance on how to protect against malicious cyber activity targeting managed service providers and their customers. This cybersecurity advisory follows a set of risk considerations issued in 2021 by CISA's National Risk Management Center, as well as CISA's guidance for small- and mid-sized businesses using managed service providers to manage IT systems, store data, or support sensitive processes. I am continuing to assess this issue with CISA and our other partners, including through the Cybersecurity Forum for Independent and Executive Branch Regulators noted above, and we are seeking to understand the extent to which agencies have developed a record on the risks posed by foreign management of United States networks. In addition, in January I announced that I intend to share with my colleagues a proposed rulemaking that would provide a framework for national security agencies to reassess a foreign carrier's authorization to provide service in the United States on an ongoing basis. As part of that rulemaking, we will also seek comment on the issues you have raised regarding the foreign management of United States telecommunications networks.

I appreciate your interest in national security and the need to evolve our policies regarding telecommunications. I would be happy to keep your office updated as we continue to work on these matters and collaborate with our national security colleagues.

Sincerely,

Jessica Rosenworcel