FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF
THE CHAIRMAN

June 15, 2017

The Honorable Ted Lieu
U.S. House of Representatives
236 Cannon House Office Building
Washington, D.C. 20515

Dear Congressman Lieu:

Thank you for your letter concerning the security of America's communications infrastructure. I agree that we must have robust and resilient communications networks and that the Commission should foster such networks consistent with its statutory authority.

The Presidential Policy Directive on Critical Infrastructure Security and Resilience (PPD-21), released in 2013, reaffirmed a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure, including infrastructure in the communications sector. The Department of Homeland Security's Office of Cybersecurity and Communications serves as the sector-specific agency responsible for overseeing the preparedness of the communications sector with respect to cybersecurity.

The role that Congress and the President have prescribed for the FCC, in contrast, is a supporting one. We are to "partner" with the Department of Homeland Security and the Department of State on "(1) identifying and prioritizing communications infrastructure; (2) identifying communications sector vulnerabilities and working with industry and other stakeholders to address those vulnerabilities; and (3) working with stakeholders, including industry, and engaging foreign governments and international organizations to increase the security and resilience of critical infrastructure within the communications sector and facilitating the development and implementation of best practices promoting the security and resilience of critical communications infrastructure on which the Nation depends."[1]

Through the Communications Security, Reliability, and Interoperability Council (CSRIC), the Commission has done just that. Last year, the Commission tasked CSRIC V with seeking ways to address security vulnerabilities within the Signaling System 7 (SS7) protocol suite including authentication and encryption of SS7 network traffic.[2] As you mention in your letter, on March 15, 2017, CSRIC V issued several recommendations to mitigate SS7 vulnerabilities.[3] Among other recommendations, the report notes that security countermeasures—including signaling interconnection monitoring and filtering and subscriber encryption support—would help to reduce SS7 security risks. We have evaluated CSRIC V's recommendations and find that their implementation would improve the security and reliability of SS7 networks. Accordingly, we plan to encourage carriers to voluntarily implement CSRIC V's recommendations on SS7 risk mitigation strategies and to monitor their implementation. CSRIC V also recommended further work should be done by CSRIC on two emerging

---

[1] White House, Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (2013).

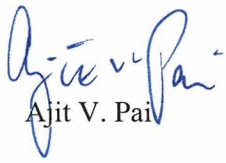
[2] *See* CSRIC Launches Group to Study Signaling System 7 Security, https://blog.npstc.org/2016/06/28/csric-launches-group-to-study-signaling-system-7-security/ (2016).

[3] *See* WORKING GROUP 10 Legacy Systems Risk Reductions Final Report, https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf (2017).

technologies: the Diameter protocol and 5G. We agree. Accordingly, we have tasked the next CSRIC, CSRIC VI, to recommend best practices to mitigate the network reliability and security risks associated with the Diameter protocol, an industry standard for connecting and authenticating subscribers on mobile networks. We have also tasked CSRIC VI to recommend mechanisms for designing and deploying 5G networks to mitigate risks to network reliability and security posed by the proliferation of Internet of Things devices and open-source software platforms used in 5G networks.

I appreciate your shared commitment to the security of our nation's communications infrastructure. I look forward to working with your office, as well as our partners at the Department of Homeland Security and the Department of State, to protect the communications sector from cyberthreats. Please let me know if I can be of any further assistance.

Sincerely,



Ajit V. Pai

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF
THE CHAIRMAN

June 15, 2017

The Honorable Ron Wyden
United States Senate
221 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Senator Wyden:

Thank you for your letter concerning the security of America's communications infrastructure. I agree that we must have robust and resilient communications networks and that the Commission should foster such networks consistent with its statutory authority.

The Presidential Policy Directive on Critical Infrastructure Security and Resilience (PPD-21), released in 2013, reaffirmed a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure, including infrastructure in the communications sector. The Department of Homeland Security's Office of Cybersecurity and Communications serves as the sector-specific agency responsible for overseeing the preparedness of the communications sector with respect to cybersecurity.

The role that Congress and the President have prescribed for the FCC, in contrast, is a supporting one. We are to "partner" with the Department of Homeland Security and the Department of State on "(1) identifying and prioritizing communications infrastructure; (2) identifying communications sector vulnerabilities and working with industry and other stakeholders to address those vulnerabilities; and (3) working with stakeholders, including industry, and engaging foreign governments and international organizations to increase the security and resilience of critical infrastructure within the communications sector and facilitating the development and implementation of best practices promoting the security and resilience of critical communications infrastructure on which the Nation depends."[1]

Through the Communications Security, Reliability, and Interoperability Council (CSRIC), the Commission has done just that. Last year, the Commission tasked CSRIC V with seeking ways to address security vulnerabilities within the Signaling System 7 (SS7) protocol suite including authentication and encryption of SS7 network traffic.[2] As you mention in your letter, on March 15, 2017, CSRIC V issued several recommendations to mitigate SS7 vulnerabilities.[3] Among other recommendations, the report notes that security countermeasures—including signaling interconnection monitoring and filtering and subscriber encryption support—would help to reduce SS7 security risks. We have evaluated CSRIC V's recommendations and find that their implementation would improve the security and reliability of SS7 networks. Accordingly, we plan to encourage carriers to voluntarily implement CSRIC V's recommendations on SS7 risk mitigation strategies and to monitor their implementation. CSRIC V also recommended further work should be done by CSRIC on two emerging

[1] White House, Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (2013).

[2] *See* CSRIC Launches Group to Study Signaling System 7 Security, https://blog.npstc.org/2016/06/28/csric-launches-group-to-study-signaling-system-7-security/ (2016).

[3] *See* WORKING GROUP 10 Legacy Systems Risk Reductions Final Report, https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf (2017).

technologies: the Diameter protocol and 5G. We agree. Accordingly, we have tasked the next CSRIC, CSRIC VI, to recommend best practices to mitigate the network reliability and security risks associated with the Diameter protocol, an industry standard for connecting and authenticating subscribers on mobile networks. We have also tasked CSRIC VI to recommend mechanisms for designing and deploying 5G networks to mitigate risks to network reliability and security posed by the proliferation of Internet of Things devices and open-source software platforms used in 5G networks.

I appreciate your shared commitment to the security of our nation's communications infrastructure. I look forward to working with your office, as well as our partners at the Department of Homeland Security and the Department of State, to protect the communications sector from cyberthreats. Please let me know if I can be of any further assistance.

Sincerely,

Ajit V. Pai