Office of the Under Secretary
National Protection and Programs Directorate
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

May 22, 2018

The Honorable Ron Wyden
United States Senate
Washington, DC 20510

Dear Senator Wyden:

Thank you for meeting with me on Thursday, May 17, 2018, to discuss your objection to Senate consideration of the President's nomination for me to serve as the Under Secretary for the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD). I appreciated the opportunity to better understand your concerns related to International Mobile Subscriber Identity (IMSI) catcher technology and your request for DHS to remove "For Official Use Only" (FOUO) from a pre-decisional presentation recently delivered by a DHS employee to an audience of federal network security professionals.

As we discussed, NPPD coordinates efforts to ensure the security, resiliency, and reliability of the Nation's cyber and communications infrastructure. We work closely with the Federal Communications Commission, law enforcement, the Intelligence Community, and private sector organizations to accomplish this mission. Our efforts are built on voluntary partnerships. Together, we provide valuable services to our partners, including facilitating information sharing and best practices, and working with telecommunications companies to identify and mitigate vulnerabilities.

With this in mind, from January 2017 to November 2017, NPPD conducted a limited pilot project that deployed sensors in the National Capitol Region (NCR) in order to identify and better understand potential IMSI catcher activity. An IMSI is a unique identification number used to recognize a mobile device on any cellular network, and IMSI catcher technology can be used to monitor and track cellular communications and devices as they communicate with networks. This technology can be used for both lawful and unlawful purposes. While the NPPD pilot did observe anomalous activity that appeared consistent with IMSI catcher technology within the NCR, including locations in proximity to potentially sensitive facilities like the White House, NPPD has neither validated nor attributed such activity to specific entities, devices, or purposes. It is my understanding that relevant law enforcement and counterintelligence agencies conducted further investigation and determined some detected signals were emanating from legitimate cell towers. As we discussed, NPPD lacks the appropriate enforcement and counterintelligence authorities to address your specific concerns with IMSI catcher technology. However, I take this matter seriously, and as promised, NPPD shared its findings with the appropriate Federal agencies.

NPPD remains active on this issue within the scope of our mission. During a February 6, 2018, meeting of the Federal Chief Information Officer Council's Mobile Technology Tiger Team (MTTT), a DHS employee presented information on communications network vulnerabilities including IMSI catcher technology as part of a broader dialogue on cellular network threats. MTTT events are intended for personnel within the Executive Branch agencies with responsibilities related to mobile policy, technology, standards, and programs. Because the presentation contained pre-decisional information and did not represent a final, validated assessment by DHS, certain slides were marked FOUO and contained further guidance that the information was not available for public release.

As we discussed during our meeting, the slides that you requested be reviewed for a public release determination are part of the pre-decisional work product of the employee-presenter, and do not constitute a validated assessment of DHS. In response to your request, and given your longstanding concerns about over-classification in the federal government, I ordered a review of these slides to assess their sensitivity and determine whether the material was appropriately marked FOUO. It is DHS's determination that the information was appropriately marked, and therefore not appropriate for public release.

While DHS is unable to release these slides publicly, we recognize the need to keep our partners and the American public informed of threats to our nation's communications networks by sharing vetted, validated information about these threats. DHS has received reports from third parties about the unauthorized use of IMSI catcher technology, as well as reports that nefarious actors may have exploited Signaling System Seven (SS7) vulnerabilities to target the communications of American citizens. Enclosed is a copy of the April 2017 DHS Study on Mobile Device Security, which addresses in detail the Department's findings on a range of communications infrastructure threats and risks, including IMSI catcher technology and SS7 vulnerabilities. This report is also available publicly at the DHS website.

Thank you again for meeting with me to discuss this issue, which I recognize is of great interest to you. Again, while NPPD does not have the law enforcement and counterintelligence authorities to pursue this issue further, NPPD has shared our findings on this topic with our Federal partners with the appropriate law enforcement and counterintelligence missions and authorities.

I hope the information provided in this letter addresses your concerns, particularly with respect to NPPD's limited role relative to any law enforcement or counterintelligence concerns related to IMSI catcher technology. I look forward to working with you in the future, and respectfully request that you allow the Senate to proceed with consideration of this nomination. Further delay in confirming DHS cybersecurity leadership only harms our nation's efforts in this and other critical areas.

If I can be of any further assistance in this matter, please do not hesitate to contact me.

Sincerely,

Christopher C. Krebs
Senior Official Performing the Duties
of the Under Secretary

Enclosure