RON WYDEN
OREGON

RANKING MEMBER OF COMMITTEE ON FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate

WASHINGTON, DC 20510-3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON BUDGET
COMMITTEE ON ENERGY & NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

September 14, 2017

The Honorable Admiral Michael S. Rogers
Director
National Security Agency
9800 Savage Rd., Suite 6272
Ft. George G. Meade, MD 20755-6000

Dear Admiral Rogers:

The Department of Homeland Security (DHS) recently published a timely and critically important report on cybersecurity threats related to mobile phones and cellular networks. In that report, DHS stated that the agency "believes that all U.S. carriers are vulnerable to [Signaling System No. 7 (SS7)] exploits, resulting in risks to national security, the economy, and the Federal Government's ability to reliably execute national essential functions." According to DHS, these "vulnerabilities can be exploited by criminals, terrorists, and nation-state actors/foreign intelligence organizations."

As the DHS report notes, the SS7 vulnerabilities can be used to "determine the physical location of cellular mobile devices, disrupt phone service from individual phones to entire networks, intercept or block SMS text messages, and redirect or eavesdrop on voice conversations."

On May 11, 2017, you testified before the Senate Select Committee on Intelligence at the annual Worldwide Threats open hearing. At that hearing, I asked you a question about SS7 and the recent DHS report. Responding to my question, you stated that you "share the concern" about SS7, but stated that you did not have specific technical knowledge about this issue, but that you would be willing to answer follow-up questions about this topic.

I would like to take you up on that offer. I would appreciate responses to the following questions by October 13, 2017, and that the responses be unclassified, to the extent possible.

1. Please describe all incidents known to NSA in which foreign governments or criminals have utilized SS7-related surveillance techniques against the employees of U.S. companies or non-profits to:
    a. Track their location.
    b. Intercept their calls or text messages.
    c. Deliver malware to their smartphones.

911 NE 11TH AVENUE
SUITE 630
PORTLAND, OR 97232
(503) 326-7525

405 EAST 8TH AVE
SUITE 2020
EUGENE, OR 97401
(541) 431-0229

SAC ANNEX BUILDING
105 FIR ST
SUITE 201
LA GRANDE, OR 97850
(541) 962-7691

U.S. COURTHOUSE
310 WEST 6TH ST
ROOM 118
MEDFORD, OR 97501
(541) 858-5122

THE JAMISON BUILDING
131 NW HAWTHORNE AVE
SUITE 107
BEND, OR 97701
(541) 330-9142

707 13TH ST, SE
SUITE 285
SALEM, OR 97301
(503) 589-4555

HTTP://WYDEN.SENATE.GOV

2. Please describe all incidents known to NSA in which foreign governments or criminals have utilized SS7 surveillance techniques against individuals in the United States, including journalists and human rights activists to:
    a. Track their location.
    b. Intercept their calls or text messages.
    c. Deliver malware to their smartphones.
3. Please describe all incidents known to NSA in which foreign governments or criminals have utilized SS7-related surveillance techniques against individuals employed by the executive, legislative or judicial branches of the U.S. government, including U.S. government negotiators and diplomats, whether in the U.S. or abroad to:
    a. Track their location.
    b. Intercept their calls or text messages.
    c. Deliver malware to their smartphones.
4. Please describe all incidents known to NSA in which foreign governments or criminals have utilized SS7-related surveillance techniques against individuals employed by any state, local, or tribal government in the United States to:
    a. Track their location.
    b. Intercept their calls or text messages.
    c. Deliver malware to their smartphones.
5. NSA publishes a number of technical documents online detailing recommended best practices to "harden" various computer systems. Are there specific technical measures that NSA believes that, if implemented, would "harden" U.S. telecommunications networks, that U.S. wireless carriers have not yet taken to protect their networks from SS7 surveillance?
6. How long has NSA been aware of the SS7-related vulnerabilities described in the DHS report?
7. NSA has a long-standing Information Assurance mission. National Security Directive 42 authorizes NSA to secure National Security Systems, which includes systems that handle classified information or are otherwise critical to military or intelligence activities. What efforts to date has NSA engaged in to protect U.S. government personnel from SS7 surveillance by foreign intelligence agencies? Has the NSA asked other agencies to protect U.S. government personnel from these types of attacks?
8. NSA has publicly stated that it regularly discloses information about security vulnerabilities to the private sector. What efforts to date has NSA engaged in to warn the private sector and the general public about SS7-related surveillance threats?
9. What actionable recommendations does NSA have for Americans, including those employed by the U.S. government, who wish to protect themselves from these threats?
10. Does NSA share DHS's assessment about the impact of SS7 vulnerabilities on U.S. national security, the economy, and the federal government and the threat posed by SS7 surveillance? If not, why?
11. Does NSA agree with DHS's assessment that all U.S. carriers are vulnerable to SS7 surveillance? If not, why?
12. Does NSA agree with DHS's assessment that SS7 vulnerabilities can be exploited by criminals, terrorists and nation-state actors/foreign intelligence organizations? If not, why?

13. As Commander of the U.S. Cyber Command, what is your view of the vulnerability of the U.S. military to SS7 surveillance? What, to date, has U.S. Cyber Command done to protect military personnel from SS7 surveillance?

If you have any questions about this this request, please contact Chris Soghoian on my staff at (202) 224-5244.

Sincerely,

Ron Wyden
United States Senator