CHARLES E. GRASSLEY, IOWA, CHAIRMAN

ORRIN G. HATCH, UTAH
JEFF SESSIONS, ALABAMA
LINDSEY O. GRAHAM, SOUTH CAROLINA
JOHN CORNYN, TEXAS
MICHAEL S. LEE, UTAH
TED CRUZ, TEXAS
JEFF FLAKE, ARIZONA
DAVID VITTER, LOUISIANA
DAVID A. PERDUE, GEORGIA
THOM TILLIS, NORTH CAROLINA

PATRICK J. LEAHY, VERMONT
DIANNE FEINSTEIN, CALIFORNIA
CHARLES E. SCHUMER, NEW YORK
RICHARD J. DURBIN, ILLINOIS
SHELDON WHITEHOUSE, RHODE ISLAND
AMY KLOBUCHAR, MINNESOTA
AL FRANKEN, MINNESOTA
CHRISTOPHER A. COONS, DELAWARE
RICHARD BLUMENTHAL, CONNECTICUT

KOLAN L. DAVIS, *Chief Counsel and Staff Director*
KRISTINE J. LUCIUS, *Democratic Chief Counsel and Staff Director*

United States Senate
COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510–6275

September 29, 2015

VIA ELECTRONIC TRANSMISSION

The Honorable Jeh Johnson
Secretary of the Department of Homeland Security
U.S. Department of Homeland Security
Washington, D.C. 20528

Dear Secretary Johnson:

Thank you for the responses you have previously provided to questions we have raised regarding the use of cell-site simulators (sometimes referred to as "IMSI Catchers" or "Stingrays") by components of the Department of Homeland Security (DHS). These devices mimic cell towers, forcing cell phones in the area to convey their approximate location and registration information. While these devices can be useful tools for identifying the location of a suspect's cell phone or identifying an unknown cell phone, they also present significant privacy concerns because they gather information about the cell phones of many people who are not investigative targets but happen to be in the vicinity.

We have previously expressed concerns about the privacy implications of these devices, as well as the inconsistent practices and policies across federal, state and local agencies that employ them. Earlier this month, the Department of Justice (DOJ) publicly issued new policy guidance governing the use of cell-site simulators by DOJ components. We are pleased that DOJ made this new guidance public; established uniform rules across its components; instituted a default warrant requirement for the use of these devices; required disclosure to reviewing courts about the way the technology works and its effect on non-target phones; and mandated deletion periods for data about non-target phones. While we remain concerned about some of the details, and in particular the potential scope of the largely undefined "exceptional circumstances" exception to the warrant requirement, we believe the DOJ guidance is a step in the right direction.

In light of reports that DHS also is working on a Department-wide policy to govern the use of cell-site simulators, we urge you to adopt a default warrant requirement, as DOJ did, but to avoid any ill-defined and potentially overbroad exceptions to that warrant requirement. We also remain concerned about the use of cell-site simulators by state and local agencies, which previously have been required to sign non-disclosure agreements when purchasing this equipment.

Accordingly, please provide responses to the following questions by no later than October 9, 2015:

1. What is the status of the DHS policy guidance review?

2. Will the Department-wide policy be public? If not, please explain why not.

3. Will the Department-wide policy establish uniform rules across its components? If not, please explain why not.

4. Will the Department-wide policy impose a default warrant requirement for the use of these devices and avoid any ill-defined and potentially overbroad exceptions? If not, please explain why not.

5. Will the Department-wide policy require the disclosure to reviewing courts about the way the technology works and its effect on non-target phones? If not, please explain why not.

6. Will the Department-wide policy mandate deletion periods for data about non-target phones? If not, please explain why not.

7. Does DHS loan cell-site simulators to state and local agencies, or provide federal grants that are used by state and local agencies to obtain cell-site simulators? If so, does DHS place any conditions on the use of those devices when purchased with federal money? If not, are there alternative methods by which DHS can incentivize state and local agencies to adopt the above-mentioned safeguards?

Also by October 9, 2015, please arrange for knowledgeable DHS officials to provide a briefing to Judiciary Committee staff that is responsive to these questions. We appreciate your assistance on this important matter.

Sincerely,

Charles E. Grassley
Chairman

Patrick Leahy
Ranking Member

cc: The Honorable Loretta Lynch
Attorney General
U.S. Department of Justice