

RON WYDEN
OREGON

223 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244
(202) 224-1280 (TDD)

United States Senate
WASHINGTON, DC 20510-3703

September 12, 2012

COMMITTEES:

COMMITTEE ON THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SUBCOMMITTEE ON PUBLIC LANDS AND FORESTS
SPECIAL COMMITTEE ON AGING
SELECT COMMITTEE ON INTELLIGENCE
COMMITTEE ON FINANCE

J. Michael Daniel
Special Assistant to the President and
Cybersecurity Coordinator
The White House

Dear Mr. Daniel:

As a senior member of the Senate Select Committee on Intelligence, I am well aware of the real danger that cyber-attacks pose to our nation's critical infrastructure. There is no doubt that foreign governments are engaged in cyber espionage, and that there are individuals and groups at home and overseas that seek to exploit network vulnerabilities for nefarious purposes. I understand that the administration is considering putting forward an executive order that aims to improve cybersecurity disciplines and I write to express my views on this important topic

I support efforts to create meaningful incentives for owners and operators of critical infrastructure to employ adequate security protocols. Such policies should make clear that they are responsible for implementing security methods proven to protect networks and they will be held liable for not taking the necessary precautions needed to protect America from harm. These policies should focus on the outcome of secure infrastructure rather than the methods by which that security is achieved. Also, the level of security sought must correlate to the risk related to any vulnerability.

In the case of interactive computer services, such as networks that facilitate commerce, provide search services, or are platforms for social networking and speech, vulnerabilities are unlikely to constitute threats to our national security. It should be clear in any executive order related to cybersecurity that there is a fundamental difference between networks that manage infrastructure critical to public safety, like energy, water, and transportation systems, and those that provide digital goods and services to the public. It would be a profound mistake to subject our growing digital economy to onerous new cyber rules and regulations that stifle innovation, creativity, and job growth. Such rules will not serve to combat the real threat to the nation's critical infrastructure and national security.

Additionally, any proposal that aims to improve cybersecurity must not undermine Americans' right to privacy or their civil liberties. Cybersecurity proposals need not license the government to unnecessarily obtain and snoop through people's electronic communication in order to combat cyber-attacks. Not only is it inherently wrong to erode privacy in the name of cybersecurity, doing so will undermine our national interest of promoting an Internet that people trust. That Internet is transforming societies, spreading democracy, and fostering new opportunities for commerce. I appreciate your consideration of my views.

Sincerely,



Ron Wyden
United States Senator

911 NE 11TH AVENUE
SUITE 630
PORTLAND, OR 97232-4169
(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](http://wyden.senate.gov)

PRINTED ON RECYCLED PAPER