COMMITTEE ON THE JUDICIARY
- *RANKING MEMBER* — SUBCOMMITTEE ON IMMIGRATION, POLICY AND ENFORCEMENT
- SUBCOMMITTEE ON INTELLECTUAL PROPERTY, COMPETITION, AND THE INTERNET

COMMITTEE ON HOUSE ADMINISTRATION
- *RANKING MEMBER* — SUBCOMMITTEE ON OVERSIGHT

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
- SUBCOMMITTEE ON ENERGY AND ENVIRONMENT
- SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT

Congress of the United States
House of Representatives
Washington, DC 20515

ZOE LOFGREN
16TH DISTRICT, CALIFORNIA

635 NORTH FIRST STREET
SUITE B
SAN JOSE, CA 95112
(408) 271-8700

1401 LONGWORTH HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-3072

WWW.HOUSE.GOV/LOFGREN

CHAIR, CALIFORNIA DEMOCRATIC CONGRESSIONAL DELEGATION

CO-CHAIR, CONGRESSIONAL CAUCUS ON VIETNAM

CO-CHAIR, DIVERSITY & INNOVATION CAUCUS

CO-CHAIR, CONGRESSIONAL HAZARDS CAUCUS

September 20, 2012

J. Michael Daniel
Special Assistant to the President
Cybersecurity Coordinator
Executive Office of the President

Dear Mr. Daniel:

Cyber attacks can pose serious threats to public safety and national security, and patching vulnerabilities in our computer networks is an urgent task. Unfortunately, Congress failed to pass a cybersecurity bill this legislative session. My understanding is that this impasse has prompted the Obama Administration to draft an executive order on cybersecurity. I am writing to urge you to specifically focus any such executive order on genuinely critical infrastructure.

The executive order should extend to the owners and operators of critical infrastructure systems, such as those that – if disrupted – could cause major economic disruption, the loss of thousands of lives, or severe degradation of national security. Targeting the executive order to critical infrastructure will allocate agency resources more efficiently, minimize conflicting regulatory requirements, and address the most acute threats to public safety.

The executive order should clearly exclude non-critical online services, such as social networking, search engines, and e-commerce networks. Imposing cybersecurity standards on non-critical systems can divert attention away from actions that are central to the functioning of American society and public safety while posing a negative impact on free expression, privacy, business operating costs, and innovation in digital services. Cybersecurity standards for non-critical systems is better addressed through a transparent legislative process that affords technical experts and the public adequate opportunity for input.

Sincerely,

Zoe Lofgren
Member of Congress