

ONE HUNDRED TWELFTH CONGRESS  
**Congress of the United States**  
**House of Representatives**  
COMMITTEE ON ENERGY AND COMMERCE  
2125 RAYBURN HOUSE OFFICE BUILDING  
WASHINGTON, DC 20515-6115

Majority (202) 225-2927  
Minority (202) 225-3641

October 4, 2011

The Honorable Gene Dodaro  
Comptroller General  
U.S. Government Accountability Office  
441 G Street, N.W.  
Washington, D.C. 20548

Dear Mr. Dodaro:

Americans are spending increasing amounts of time on the Internet and increasingly are doing so through the use of smartphones and tablets. Small businesses are taking advantage of the Internet's low barriers to entry to explore new markets, and many companies are now trying to leverage the scope and scale of cloud computing to improve the efficiency of their operations. The federal government is similarly offering more services over the Internet, and states have used online tools to make routine interactions, such as vehicle registration, more accessible. Public safety agencies at all levels of government similarly are deploying advanced communications networks that connect to the Internet. More generally, there is a surge across the country in the use of Internet Protocol (IP) based technology.

As online and IP-based communications increase, however, so do the threats of malware, cybercrime, and cyberwarfare. Cyberattacks can create costly and debilitating problems, interrupt commerce, undermine confidence in broadband communications networks, and raise public safety and national security concerns. Securing cyberspace is no easy task. Every effort should be made to reduce vulnerabilities and prevent cyberattacks. At the same time, we should maximize opportunities to encourage investment, competition, and innovation in the evolving communications marketplace. We should seek a balanced approach that capitalizes on commercial sector expertise in conjunction with government efforts to address cyberthreats.

Furthermore, we need to address the provision by non-U.S. vendors of hardware and software for incorporation into communications networks. In this regard, we need to be mindful of enabling industry participants to gain access to low-cost, high-quality equipment while protecting against vendors that may seek to undermine cybersecurity by introducing harmful

network components or software into our nation's communications networks, whether for purposes of surveillance, disruption, deception, or destruction.

Accordingly, we request that the Government Accountability Office (GAO) examine the following important aspects of cybersecurity:

#### The Role of Federal Agencies in Cybersecurity

- Given the respective roles of the Federal Communications Commission (FCC), the National Telecommunications and Information Administration (NTIA), and the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC) and Office of Emergency Communications (OEC), what actions have these agencies taken to address the cybersecurity challenges to communications networks? What roles have the FCC's Communications Security, Reliability and Interoperability Council and the NTIA's Internet Policy Task Force played?
- How are these agencies leveraging the capabilities of the commercial sector to bolster their own cybersecurity efforts? How are they assessing and assisting the cybersecurity practices of private-sector communications companies and Internet Service Providers? What actions are these agencies taking or considering to ensure that smart grids and the communications equipment and services used to enable such networks are secure?
- How are these agencies working with state and local governments, including first responder agencies, emergency operations centers, and public safety answering points, to coordinate their cybersecurity efforts?
- Is the Defense Industrial Base Cyber Pilot a viable model for these agencies to follow in promoting cybersecurity in the communications and Internet sectors?
- What additional efforts should these agencies undertake to promote cybersecurity?

#### The Protection and Security of Consumer Communications Products and Services

- What security features are included in the hardware and software of commonly available modems, routers, cellphones, smartphones, and tablets? What role do wired and wireless communications providers and equipment vendors play in determining the security of such services and devices? How do the cybersecurity protections vary among the different communications technologies?
- What, if any, widespread or systematic vulnerabilities exist, and how are they being mitigated by private-sector or governmental action?
- To what extent have security problems, such as hacked communications networks or wireless transmissions, been reported to government agencies and what consequences, such as identity theft, have arisen from these problems? What reporting and disclosure requirements or structures are currently in place?

#### The Security and Oversight of Equipment in Communications Networks

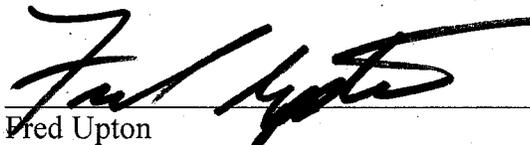
- Who are the main non-U.S. suppliers of hardware and software for commercial and public safety communications networks in the United States? How large a role do these suppliers play in the U.S. market?

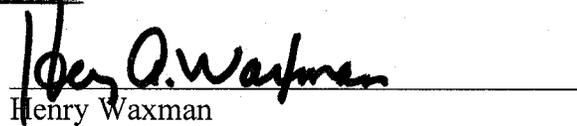
- How are non-U.S. vendor hardware and software used as core components of commercial and public safety communications networks in the United States?
- How does the government and private sector evaluate the benefits and risks associated with proposals by non-U.S. vendors to supply core hardware and software for commercial and public safety communications networks in the United States?
- When non-U.S. companies propose to purchase certain U.S. assets, the Committee on Foreign Investment in the United States conducts a formalized review. What are the advantages and disadvantages of such a process, and could such a process provide a template on which to formalize review of certain purchases by U.S. communications companies of non-U.S. vendor hardware and software for use as core components of networks?

In addition, we request that GAO inform the Committee regarding any other issues of concern that it may uncover during its examination of these issues.

Thank you for your attention to this request. If you have any questions about this request, please have your staff contact Neil Fried or Nick Degani at (202) 225-2927.

Sincerely,

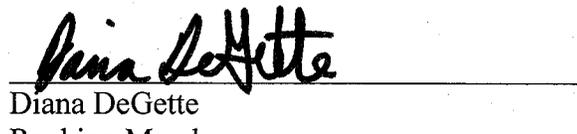
  
Fred Upton  
Chairman

  
Henry Waxman  
Ranking Member

  
Greg Walden  
Chairman, Subcommittee on  
Communications and Technology

  
Anna Eshoo  
Ranking Member, Subcommittee on  
Communications and Technology

  
Cliff Stearns  
Chairman  
Subcommittee on Oversight and  
Investigations

  
Diana DeGette  
Ranking Member  
Subcommittee on Oversight and  
Investigations

cc: Chairman Julius Genachowski, Federal Communications Commission  
Commissioner Michael Copps, Federal Communications Commission  
Commissioner Robert McDowell, Federal Communications Commission  
Commissioner Mignon Clyburn, Federal Communications Commission

Assistant Secretary Larry Strickling, National Telecommunications and Information  
Administration, Department of Commerce

Director Seán McGurk, National Cybersecurity and Communications Integration Center,  
Department of Homeland Security

Director Chris Essid, Office of Emergency Communications, Department of Homeland  
Security