Question#:	1
Topic:	proposal
Hearing:	Cybersecurity: Evaluating the Administration's Proposals
Primary:	The Honorable Sheldon Whitehouse
Committee:	JUDICIARY (SENATE)

Question: Under the Administration's proposal, a rulemaking process would identify critical infrastructure in the United States. Current legislative discussions presume that the electrical grid and certain other pieces of infrastructure will be determined to be critical in such a rulemaking process. Internet Service Providers (ISPs) would appear to be an essential element of our infrastructure and economy. Should Congress expect ISPs (or elements thereof) to be identified as critical infrastructure under the proposed rulemaking process?

Response: The Administration's cybersecurity legislative proposal does not specify which infrastructure will be designated as "covered critical infrastructure" and instead opts for an inclusive and transparent rulemaking process to develop the list. It is premature to commit to which items will or will not be included in a proposed rulemaking.

Question#:	2
Topic:	ISPs
Hearing:	Cybersecurity: Evaluating the Administration's Proposals
Primary:	The Honorable Sheldon Whitehouse
Committee:	JUDICIARY (SENATE)

Question: Would the Administration's proposal and anticipated regulations enable or require ISPs to notify customers that they are the unwitting and unwilling bearers of viruses, malware and other threats?

Response: The Administration understands that some internet service providers (ISPs) have already begun pilot projects to better inform customers regarding intrusions into their networks. Although the Department of Homeland Security is supportive of ISPs working with their customers on a voluntary basis to enhance the security of the entire digital ecosystem, the Administration's proposal is silent on the particular issue of ISPs sharing information with customers or other private sector entities to inform them that they are subject to malware or other cybersecurity threats. To the extent that such information sharing is currently permissible, it would continue to be so under the proposal. We look forward to working with the Chairman and members of the Committee to determine if additional action should be taken to encourage this type of assistance.

Question: What steps would the Administration propose to customers whose computers are bearers of viruses, malware, and other threats, particularly to those unwilling to take reasonable remedial and protective steps?

Response: Within the National Protection and Program Directorate's Office of Cybersecurity and Communications, the U.S. Computer Emergency Readiness Team provides government agencies, the private sector, and the general public with suggested cybersecurity best practices and vulnerability and mitigation information. Internet service provider (ISP) customers are encouraged to regularly update anti-virus software, download vendor security patches, and exercise caution when using removable media, following links, or opening email attachments. If an ISP customer is unwilling to implement these remedial and protective steps, those customers should be made aware of the potential associated consequences, such as identity theft, financial fraud, privacy concerns, and the theft of other types of data. ISP customers should be aware of consequence-management resources available to them, such as credit and bank account monitoring, and should also consider limiting the amount of personal information stored or accessed from their computers.