

ONE HUNDRED SEVENTEENTH 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

August 30, 2021

Ms. Kemba Walden  
Assistant General Counsel  
Microsoft Corporation  
One Microsoft Way  
Redmond, WA 98052

Dear Ms. Walden:

Thank you for appearing before the Subcommittee on Oversight and Investigations on Wednesday, July 20, 2021, at the hearing entitled “Stopping Digital Thieves: The Growing Threat of Ransomware.” I appreciate the time and effort you gave as a witness before the Committee on Energy and Commerce.

Pursuant to Rule 3 of the Committee on Energy and Commerce, members are permitted to submit additional questions to the witnesses for their responses, which will be included in the hearing record. Attached are questions directed to you from certain members of the Committee. In preparing your answers to these questions, please address your response to the member who has submitted the questions in the space provided.

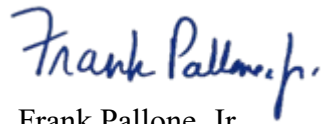
To facilitate the printing of the hearing record, please submit your responses to these questions no later than the close of business on Monday, September 13, 2021. As previously noted, this transmittal letter and your responses will all be included in the hearing record. Your written responses should be transmitted by e-mail in the Word document provided to Austin Flack, Policy Analyst, at [austin.flack@mail.house.gov](mailto:austin.flack@mail.house.gov). To help in maintaining the proper format for hearing records, please use the document provided to complete your responses.

Ms. Kemba Walden

Page 2

Thank you for your prompt attention to this request. If you need additional information or have other questions, please contact Austin Flack with the Committee staff at (202) 225-2927.

Sincerely,

A handwritten signature in blue ink that reads "Frank Pallone, Jr." in a cursive style.

Frank Pallone, Jr.  
Chairman

Attachment

Ms. Kemba Walden

Page 3

cc: The Honorable Cathy McMorris Rodgers  
Ranking Member  
Committee on Energy and Commerce

The Honorable Diana DeGette  
Chair  
Subcommittee on Oversight and Investigations

The Honorable H. Morgan Griffith  
Ranking Member  
Subcommittee on Oversight and Investigations

**Attachment—Additional Questions for the Record**

**Subcommittee on Oversight and Investigations  
Hearing on  
“Stopping Digital Thieves: The Growing Threat of Ransomware”  
July 20, 2021**

Ms. Kemba Walden, Assistant General Counsel, Microsoft Corporation

**The Honorable Frank Pallone, Jr. (D-NJ)**

1. The Department of Homeland Security, FBI, and other law enforcement assist with incident response, but I would like to understand whether we are providing victims the variety of resources needed beyond traditional law enforcement, such as technical expertise, recovery strategies, best practices on how to deal with the malicious actors, and other resources that may be required in order to ensure continuity of operations.
  - a. What more do you think the U.S. government can and should be providing to victims of ransomware attacks?
  - b. Do you have any recommendations for actions Congress may take in order to assist in those efforts?

**The Honorable Diana DeGette (D-CO)**

1. I am encouraged by the actions the Biden Administration has taken thus far, including the announcement of forthcoming cybersecurity performance goals for critical infrastructure and the formalization of the Industrial Control System Cybersecurity Initiative. Given the critical role the private sector plays in both the operation and security of our critical infrastructure, I would like to hear your take on its response to these threats and to the initiatives and requirements being announced by DHS and other agencies. How do you rate private industry’s response thus far and is there anything Congress can be doing to further incentivize the private sector to take these threats seriously?

**The Honorable H. Morgan Griffith (R-VA)**

1. The first ransomware attack occurred in 1989, it is not a new threat, but a longstanding cybercrime. The new aspect of ransomware is the use of cryptocurrencies for ransom payments. Can you explain how the role of cryptocurrencies has changed the nature of ransomware attacks?

**The Honorable Gary Palmer (R-AL)**

1. Unfortunately, many of these attacks abuse the fact that corporate networks run on Microsoft software. Every ransomware actor seeks to gain “Domain Admin” level control as the first step to being able to adjust “Global Policies” in the Windows Registry to enable the encryption and exfiltration of the entire network. Is there more that Microsoft could be doing to detect and stop unauthorized Powershell commands or changes to Global Policies on a Windows Domain?