

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

Christian Dameff, M.D., M.S.  
Assistant Professor of Emergency Medicine, Biomedical Informatics,  
and Computer Science (Affiliate)  
University of California San Diego  
Medical Director of Cybersecurity  
UC San Diego Health  
UC San Diego Health, Department of Emergency Medicine  
200 West Arbor Drive, #8676  
San Diego, CA 92103

Dear Dr. Dameff:

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.

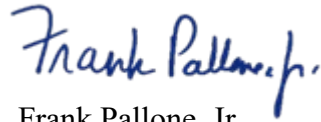
To facilitate the printing of the hearing record, please submit your responses to these questions no later than the close of business on Monday, September 13, 2021. As previously noted, this transmittal letter and your responses will all be included in the hearing record. Your written responses should 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.

Christian Dameff, M.D., M.S.

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

Christian Dameff, M.D., M.S.

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**

Christian Dameff, M.D., M.S., Assistant Professor of Emergency Medicine, Biomedical Informatics, and Computer Science (Affiliate), University of California San Diego, Medical Director of Cybersecurity, UC San Diego Health

**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 Michael C. Burgess, M.D. (R-TX)**

1. We have witnessed an uptick in ransomware attacks on health systems, especially as our nation responded to the Coronavirus public health emergency. As you highlighted

in your testimony, ransomware attacks on health systems are unique and particularly delicate as patients' private and sensitive health data is at risk, in addition to patient access to care.

- a. If larger health systems are not equipped to protect against ransomware attacks, how can smaller hospitals and health systems ensure their patients are protected?
2. Dr. Christian Dameff, during the hearing, we discussed that some organizations and hospitals may be fearful of reporting ransomware and other cyber-attacks because they do not want to lose the trust and confidence of their customers or patients.
    - a. What is the right balance to strike between requiring private entities to report ransomware or other cyber-attacks and maintaining public confidence in an affected entity's care or services?
      - i. Follow-up: Would a delayed public disclosure, required only after immediate response and recovery efforts, encourage entities to report attacks?
    - b. How can the federal government help better prepare health care organizations to prevent and respond to ransomware attacks?

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

1. In your testimony you referenced the attack on five large hospitals in the San Diego area. Did anyone die as a result of that attack?
2. I wanted to thank you for your discussion of the Software Bill of Materials (SBOM) concept. The idea, as I understand it, is that each software package a hospital installs may contain underlying vulnerabilities that the hospital is unaware of because they don't know that the vulnerable software is part of the system they purchased and installed. What could our committee, or the Congress as a whole, do to encourage the adoption of SBOM. Are you asking for Regulation? Or is this something that the FDA who has oversight over medical devices, or HHS who has oversight over compliance with HIPAA, should address through Guidance?