FEDERAL ELECTION COMMISSION
Washington, DC 20463

MEMORANDUM

TO: **The Commission**

FROM: **Office of Commission Secretary** LCS

DATE: **December 12, 2018**

SUBJECT: ***Ex Parte* Communication Concerning Advisory Opinion Request 2018-15 (Wyden)**

Transmitted herewith is a notification regarding a phone conversation by Commissioner Steven T. Walther regarding the above matter which is on the December 6, 2018 Open Meeting Agenda.

Attachments

RECEIVED
FEDERAL ELECTION COMMISSION
SECRETARIAT
2018 DEC 12 PM 3:10

FEDERAL ELECTION COMMISSION
Washington, D.C. 20463

MEMORANDUM

TO: Dayna Brown
Secretary to the Federal Election Commission

FROM: Steven T. Walther Sent by TJA
Commissioner

DATE: December 12, 2018

RE: Ex parte communication

On Tuesday, December 11, 2018, I had a phone conversation regarding Advisory Opinion Request (AOR) 2018-15 (Wyden) with Chris Soghoian, Senior Advisor for Privacy & Cybersecurity for Senator Ron Wyden. Mr. Soghoian was in Senator Wyden's office at the time, while I was in a conference room at the Federal Election Commission on speakerphone. Also present in the conference room with me were Office of General Counsel attorney Joanna Waldstreicher and a member of my staff, Executive Assistant Thomas Andersen. The information below constitutes a summary of what I understood to be Mr. Soghoian's responses to some questions I had concerning the AOR.

Concerning the range of potential expenses, Mr. Soghoian stated that the cybersecurity measures anticipated in the AOR would be mostly preventative in nature, which would be less expensive than remediation measures. He noted, however, that Senators may lack the technical expertise to implement preventative measures themselves. For example, while they could purchase a more secure router, they might need to hire an expert to set it up. He likened this to a Senator using campaign funds to hire a consultant, to the extent permitted by AO 2017-07 (Sergeant at Arms), to provide advice on improving the Senator's home security system. He noted, however, that in the rare case where a Senator's personal device or account is hacked, hiring an expert to remediate the issue could be quite expensive.

Mr. Soghoian also addressed the issue of the unique cybersecurity threat faced by elected officials, as opposed to the general public. The general public may be subject to crimes of opportunity, such as a hacker trying to steal financial information. Elected officials, however, may be specifically targeted for valuable information that could include, e.g., sensitive

communications, photos, and location information. He noted that this particular AOR is intended to apply only to the protection of elected officials, and not to family members or others.

Mr. Soghoian was asked about the status of the bipartisan Senators' Personal Cybersecurity Working Group established by the Legislative Branch Appropriations Act of 2018 to identify and recommend options for protecting Senators' personal communications devices and accounts. He responded that the Working Group has just completed its report, but that it has not been made public and he has not yet read it. He also noted that Senator Wyden plans to introduce legislation "in the new year" to address these issues.

* * *

Pursuant to 11 CFR 201.4(a), please place this summary in the public file of this advisory opinion.