

MARCO RUBIO, FLORIDA  
RON JOHNSON, WISCONSIN  
CORY GARDNER, COLORADO  
MITT ROMNEY, UTAH  
LINDSEY GRAHAM, SOUTH CAROLINA  
JOHNNY ISAKSON, GEORGIA  
JOHN BARRASSO, WYOMING  
ROB PORTMAN, OHIO  
RAND PAUL, KENTUCKY  
TODD YOUNG, INDIANA  
TED CRUZ, TEXAS

ROBERT MENENDEZ, NEW JERSEY  
BENJAMIN L. CARDIN, MARYLAND  
JEANNE SHAHEEN, NEW HAMPSHIRE  
CHRISTOPHER A. COONS, DELAWARE  
TOM UDALL, NEW MEXICO  
CHRISTOPHER MURPHY, CONNECTICUT  
TIM KAINE, VIRGINIA  
EDWARD J. MARKEY, MASSACHUSETTS  
JEFF MERKLEY, OREGON  
CORY A. BOOKER, NEW JERSEY

## United States Senate

COMMITTEE ON FOREIGN RELATIONS

WASHINGTON, DC 20510-6225

November 19, 2019

Michael T. Evanoff  
Assistant Secretary  
Bureau of Diplomatic Security  
U.S. Department of State  
2201 C Street, N.W.  
Washington, D.C. 20520

Dear Assistant Secretary Evanoff,

I write today to raise grave concerns about the use of unsecure personal telecommunication devices by senior officials of the Department to conduct sensitive national security business and to request an investigation by the Bureau of Diplomatic Security into these allegations, including, if warranted, appropriate disciplinary action. As the senior Diplomatic Security professional at the State Department, you are responsible for the Department's information security and counter-intelligence missions. I assume you share my alarm.

Testimony during the House's impeachment inquiry last week revealed that U.S. Ambassador to the European Union, Gordon Sondland, conducted a highly sensitive conversation with the President of the United States using his personal cell phone. As he made the call, he was at lunch on the terrace of a restaurant in Kyiv, Ukraine with embassy staffers and Ukrainians present and well within earshot. This incident is a serious security breach that raises significant counterintelligence concerns as well as concerns about State management of information security issues more generally. In an area of the world where kompromat, "compromising information," is a political norm, with longstanding and sophisticated roots, this episode is staggering in its recklessness.

I am sure you recall the embarrassment, political fallout, and official U.S. apology that followed the February 2014 YouTube release of the telephone call of a Department of State Assistant Secretary, a call that was intercepted in Ukraine, and that you appreciate the national security import of this breach and share my deep concern.

More troubling, Ambassador Sondland's security breaches are not isolated. Numerous other reports allege widespread use of personal cell phones as a regular means to communicate on highly sensitive matters among and between numerous senior State Department political appointees of the current administration, as well as between those officials and other officials elsewhere in the U.S. government, including President Trump himself.

I recognize that determinations about the appropriate use of communication equipment as well as the sensitivity of information under discussion can be complex and subjective. However, given the importance of this issue and the apparent culture of indifference to classification matters and

information security emanating from President Trump, I request your office immediately undertake a review of communication security at the Department—including the use of personal cell phones—by all political appointees at the Department of State, assess any security breaches, incidents or infractions, make recommendations, and take appropriate disciplinary action.

I would appreciate a response laying out your plans to investigate this matter, including scope and timeline, by December 2, 2019. Thank you for your attention to this matter and I look forward to your prompt response.

Sincerely,

A handwritten signature in blue ink that reads "Robert Menendez". The signature is fluid and cursive, with a large initial "R" and "M".

Robert Menendez  
Ranking Member