

AMY KLOBUCHAR, MINNESOTA  
RICHARD BLUMENTHAL, CONNECTICUT  
BRIAN SCHATZ, HAWAII  
EDWARD MARKEY, MASSACHUSETTS  
GARY PETERS, MICHIGAN  
TAMMY BALDWIN, WISCONSIN  
TAMMY DUCKWORTH, ILLINOIS  
JON TESTER, MONTANA  
KYRSTEN SINEMA, ARIZONA  
JACKY ROSEN, NEVADA  
BEN RAY LUJÁN, NEW MEXICO  
JOHN HICKENLOOPER, COLORADO  
RAPHAEL WARNOCK, GEORGIA

ROGER WICKER, MISSISSIPPI  
JOHN THUNE, SOUTH DAKOTA  
ROY BLUNT, MISSOURI  
TED CRUZ, TEXAS  
DEB FISCHER, NEBRASKA  
JERRY MORAN, KANSAS  
DAN SULLIVAN, ALASKA  
MARSHA BLACKBURN, TENNESSEE  
TODD YOUNG, INDIANA  
MIKE LEE, UTAH  
RON JOHNSON, WISCONSIN  
SHELLEY MOORE CAPITO, WEST VIRGINIA  
RICK SCOTT, FLORIDA  
CYNTHIA LUMMIS, WYOMING

DAVID STRICKLAND, STAFF DIRECTOR  
JOHN KEAST, REPUBLICAN STAFF DIRECTOR

# United States Senate

COMMITTEE ON COMMERCE, SCIENCE,  
AND TRANSPORTATION

WASHINGTON, DC 20510-6125

WEBSITE: <https://commerce.senate.gov>

May 17, 2021

The Honorable Alejandro Mayorkas  
Secretary of Homeland Security  
Washington, DC 20528

Dear Secretary Mayorkas:

I write to express my concern regarding the recent ransomware attack on the Colonial Pipeline Company. Today's increasingly connected world has brought great benefits and economic growth, but has also made some of our nation's pipelines, electricity grid, and transportation systems vulnerable to attack. Having nearly half of the East Coast's fuel supply crippled by a single ransomware incident highlights the urgent need to harden our nation's critical infrastructure against computer errors, criminals, and hostile foreign adversaries.

In December 2018, House Energy and Commerce Chairman Pallone and I wrote to former Secretary Nielson to express our concerns about weaknesses in the Transportation Security Administration's (TSA) pipeline security management, which were detailed in a U.S. Government Accountability Office's (GAO) report we had requested. The report concluded TSA's inadequate staffing, outdated risk assessments, a lack of information sources on current threats, and ambiguity in security standards are significant weaknesses that hampered TSA's ability to adequately oversee the nation's 2.7 million miles of pipelines. It is extremely concerning that several of the GAO's recommendations remain open, and I ask that you provide a status update on TSA's action to address them.

In that letter, I also questioned the TSA's voluntary cybersecurity standards, and requested information about what percentage of pipeline operators were fully complying with those voluntary standards. TSA indicated that of the 23 corporate security reviews it completed of pipeline operators in fiscal year 2018, 80 percent were compliant with the voluntary standards. The Colonial Pipeline Company attack and the consequential impacts that continue to unfold indicate that until we have 100 percent compliance across the industry we remain vulnerable. At a minimum, the TSA must do more to ensure that all operators achieve full compliance and should seriously consider making these voluntary standards mandatory to ensure that compliance.

As Chair of the Commerce Committee, I will be holding a hearing to further review the federal response to this cyberattack on Colonial Pipeline Company to examine what additional actions must be taken to further strengthen America's cybersecurity defenses and better protect our nation's critical infrastructure. This includes the Department's coordination with other agencies, including the Department of Energy, the Federal Energy Regulatory Commission, and the Pipeline and Hazardous Materials Safety Administration which all have key roles in this area.

Thank you for your attention to this request and I look forward to your prompt reply.

Sincerely,



Maria Cantwell

Chair