STEVE DAINES
MONTANA

320 HART SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-2651

United States Senate
WASHINGTON, DC 20510-2606

COMMITTEES
APPROPRIATIONS
ENERGY AND NATURAL RESOURCES
FINANCE
INDIAN AFFAIRS

June 15, 2021

The Honorable Janet Yellen
Secretary
U.S. Department of the Treasury
1500 Pennsylvania Avenue, NW
Washington, D.C. 20220

Dear Secretary Yellen:

In light of the recent wave of cyberattacks impacting both private companies and government entities, I write today requesting an update on Treasury's cyber infrastructure and general security in the face of ongoing threats. This is a particularly pressing issue, and I am concerned that it is not receiving the level of attention it deserves.

In recent months, we have seen a number of troubling, high-profile cyber and ransomware attacks targeting U.S. companies. Last month, a ransomware attack targeting Colonial Pipeline Co. forced the company to halt operations, resulting in fuel shortages across the southeastern United States. Earlier this month, a ransomware attack against JBS USA Holdings, Inc. halted operations at some of the largest meatpacking plants in the United States. On June 1, Scripps Health announced that, due to a May ransomware attack, hackers had stolen personal data from nearly 150,000 individuals. On June 11, McDonald's Corp. told employees that hackers had successfully stolen company data, including employee information, from its systems in the United States, South Korea, and Taiwan. Hackers have also recently targeted local entities like ferry services in Massachusetts and water treatment plants in Florida, suggesting that multinational corporations and national governments are not the only entities subject to the threat of cyber and ransomware attacks. Unfortunately, the above instances of successful cyber and ransomware attacks undoubtedly represent a small fraction of total attempts to violate the cybersecurity of U.S. corporations, government agencies, and other entities.

In December of last year, it was revealed that the Treasury Department was among the agencies impacted by the SolarWinds hack, one of the worst data breaches in the history of the United States. It is clear that cybercriminals, including those responsible for the SolarWinds hack, have continued unabated and that further action is needed to bolster Treasury's cybersecurity. This is particularly true in the wake of the unauthorized disclosure of confidential taxpayer data published by ProPublica. Luckily, the recent wave of cyber and ransomware attacks does not appear to have targeted U.S banks, stock market exchanges, mutual and pension funds, federal government agencies, or other elements critical to the operations of the U.S. financial system. However, that does not mean that U.S. financial infrastructure is immune to attack. In fact, in recent years we have seen attacks successfully target foreign central banks. In 2016, hackers installed malware on the Bangladesh Central Bank's computer system resulting in the theft of approximately $81 million.

STEVE DAINES
MONTANA

320 HART SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-2651

United States Senate
WASHINGTON, DC 20510-2606

COMMITTEES
APPROPRIATIONS
ENERGY AND NATURAL RESOURCES
FINANCE
INDIAN AFFAIRS

The U.S. financial system is a critical component of U.S. infrastructure. The industry holds trillions in assets and massive amounts of American citizens' personal data. As criminals grow more sophisticated and increasingly target ransomware attacks against U.S. critical infrastructure, the federal government must ensure that its defensive capabilities match the changing threat environment.

With that in mind, I have several questions for which I am hopeful you can provide clarification:

- How confident is Treasury that U.S. financial infrastructure is capable of preventing cyber and ransomware attacks from increasingly sophisticated criminals?
- What steps has Treasury recently taken to secure the cybersecurity of U.S. financial infrastructure?
- Has Treasury determined the full extent of the SolarWinds hack? If not, could additional sanctions be considered if additional perpetrators are identified?

The U.S. financial system relies in large part upon the security of confidential data housed at the Treasury Department. As criminals grow more sophisticated and increasingly target ransomware attacks against U.S. critical infrastructure, the federal government must ensure that its defensive capabilities match the changing threat environment. Thank you for your work to protect the integrity of U.S. financial infrastructure, and I look forward to receiving your answers to the above questions.

Sincerely,

Steve Daines
United States Senator