

# United States Senate

WASHINGTON, DC 20510

October 2, 2020

The Honorable Betsy DeVos  
Secretary  
U.S. Department of Education  
400 Maryland Avenue, SW  
Washington DC, 20202

The Honorable Chad Wolf  
Acting Secretary  
U.S. Department of Homeland Security  
245 Murray Lane SW  
Washington, DC 20528

Dear Secretary DeVos and Acting Secretary Wolf,

We write to share our concerns with the recent cyberattack at Clark County School District (CCSD) and urge the Department of Education (ED) and the Department of Homeland Security (DHS) to provide adequate support, guidance, and resources to help CCSD respond to the attack and prevent future ones. We also request that you address several questions about your respective departments' current practices to prevent and respond to cyberattacks on schools and school districts.

On August 27, a hacker subjected CCSD – Nevada's largest school district and our country's fifth largest school district, serving more than 320,000 students – to a ransomware attack. Last week, the Wall Street Journal reported that, after demanding a ransom, the hacker published documents online containing sensitive information, including employee Social Security numbers, and student names, addresses, and grades. This is unacceptable and requires an immediate federal response.

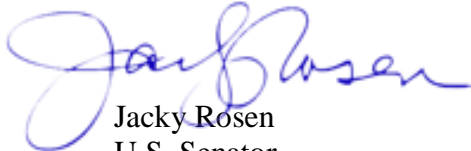
Earlier this spring, the FBI warned that K-12 institutions “represent an opportunistic target” to hackers as many school districts lack the budget and expertise to dedicate to network integrity. Cyberattacks can be expensive and debilitating, especially for small organizations or public entities, such as schools and school districts. During the COVID-19 pandemic, the number of cyberattacks and ransomware attacks have significantly increased. Elementary and secondary schools in particular face myriad threats as they transition to online learning, including constrained budgets, bridging the digital divide, ensuring the health and safety of students and faculty, and continuing to educate and support our students. The Federal government must help elementary and secondary schools obtain the tools and resources to protect and combat cyber threats.

In light of these concerns, please provide answers to the following questions no later than October 15, 2020:

1. How are your departments currently addressing cyberattacks – including ransomware attacks – against K-12 schools and school districts? What steps are you taking to ensure such attacks do not take place or lead to significant data breaches in the future?
2. Are there any current grant programs or initiatives at ED or DHS designed to assist elementary and secondary schools with implementing strong cybersecurity standards and protocols?
  - a. If so, will you provide support to CCSD and those impacted by the recent ransomware attack?
3. Do you offer guidance or support regarding ransomware attacks to elementary and secondary schools, school districts, or state education agencies, including information about cyber insurance, where they should report a cybersecurity incident, and how to identify the individuals who are impacted by incidents?
4. Do you collect data on the number of cyberattacks targeting elementary and secondary schools or school districts?
  - a. If so, how many attacks occurred in Fiscal Year 2020, and has the number of attacks increased in recent years? Has there been an uptick in attacks during the course of the COVID-19 pandemic? Has the practice of distance learning impacted the number of attacks?
5. How do you promote existing federal cyber guidance or frameworks to elementary and secondary schools?
6. Do you conduct outreach to elementary and secondary schools and school districts so they are aware of available resources, cyber prevention guidance, or tools before and after a cyber-attack?
7. Is there interagency collaboration between DHS and ED to protect elementary and secondary schools from cybersecurity attacks?
  - a. Do you partner on preventing and mitigating cyber-attacks on schools and school districts with other relevant agencies, such as the National Institute of Standards and Technology (NIST), which has had a leadership role in developing the Cybersecurity Framework?

Given the increase in cyberattacks during this pandemic, and specifically the cyberattack on CCSD in our home state of Nevada, we urge ED and DHS to take immediate action to respond to these attacks and help our schools, school districts, students, and teachers. Thank you for your attention and for your prompt response.

Sincerely,



Jacky Rosen  
U.S. Senator



Catherine Cortez Masto  
U.S. Senator