

United States Senate

WASHINGTON, DC 20510

The Honorable Kristi Noem
Secretary of Homeland Security
U.S. Department of Homeland Security
Washington, D.C. 20528

August 22, 2025

Dear Secretary Noem:

We write to express deep concern about the weakening of the Cybersecurity and Infrastructure Security Agency (CISA) and its diminishing role in supporting state and local election officials—particularly in light of the recent cyberattack targeting Arizona’s statewide candidate portal.¹

The defacement of candidate profiles with images of Iranian leadership—following U.S. military actions in the region—has raised serious questions about the capacity of foreign adversaries to disrupt American democratic processes.² While Arizona election officials moved swiftly to contain the breach, it is deeply troubling that the state did not feel it could rely on CISA for rapid, coordinated support in responding to the incident.

Until recently, CISA served as a trusted federal partner to election officials, offering threat intelligence, technical assistance, and incident response. We have heard firsthand from Arizona officials that this trust has eroded. Officials describe a dramatic reduction in support, staffing, and communication from CISA, as well as a lack of confidence in the agency’s ability to collaborate in good faith on election security.

Meanwhile, jurisdictions are increasingly concerned about CISA’s move to defund the Multi-State Information Sharing and Analysis Center (MS-ISAC)—a critical resource for cyber threat monitoring and mitigation. We are alarmed that local officials are now being asked to pay to maintain access to tools that were previously federally supported.

Cybersecurity must remain a nonpartisan, whole-of-government priority—especially when it comes to securing our elections. The apparent politicization of CISA and withdrawal of essential

¹ *Iranian Cyberattack Targeted Arizona Candidate Photos on Election Website*, *Homeland Security Today*, July 21, 2025, <https://www.hstoday.us/subject-matter-areas/cybersecurity/iranian-cyberattack-targeted-arizona-candidate-photos-on-election-website/>.

² Jen Fifield, “*Hackers who breached Arizona election website aimed at other targets, too*,” *Arizona Mirror*, July 23, 2025, <https://azmirror.com/2025/07/23/hackers-who-breached-arizona-election-website-aimed-at-other-targets-too/>.

resources comes at a time when threats to election infrastructure, disinformation campaigns, and foreign interference efforts are growing in both sophistication and scale.

We respectfully request a response to the following:

1. What steps has DHS taken to rebuild CISA's trust and operational engagement with state and local election officials, particularly in Arizona?
2. What resources or personnel were deployed to support Arizona's response to the recent cyberattack?
3. Does DHS intend to restore the staffing, technical programs, and regional infrastructure that allowed CISA to be an effective election security partner prior to 2024?
4. What is DHS's current plan to ensure continuity in election threat monitoring, rapid incident response, and secure communication channels with all 50 states?
5. Does DHS still consider election systems to be critical infrastructure?
6. What is the current funding status of the MS-ISAC, and does DHS plan to ensure continued access for state and local election officials?

We would welcome the opportunity to discuss how DHS can strengthen coordination with Arizona officials ahead of future election cycles. Protecting our election infrastructure must be above politics. We look forward to your response and to a renewed federal commitment to securing the cybersecurity of our democracy.

Sincerely,



Ruben Gallego
United States Senator



Mark Kelly
United States Senator