

## Greg Ensell

---

**From:** Greg Ensell  
**Sent:** Thursday, February 5, 2026 10:35 AM  
**To:** 'dfarnsworth@azleg.gov'; 'David Livingston'  
**Cc:** 'Ben Henderson'; 'Richard Stavneak'; 'LAUSTIN@azleg.gov'; 'SBLATTMAN@azleg.gov'; 'MCARBONE@azleg.gov'; 'MGRESS@azleg.gov'; 'JOLSON@azleg.gov'; 'SSTAHLHAMILTON@azleg.gov'; 'MWAY@azleg.gov'; 'LALSTON@azleg.gov'; 'BFERNANDEZ@azleg.gov'; 'MFINCHEM@azleg.gov'; 'JKAVANAGH@azleg.gov'; 'LKUBY@azleg.gov'; 'JMESNARD@azleg.gov'; 'CWERNER@azleg.gov'; 'Micaela Larkin Andrews'; 'Fletcher Montzingo'; 'Josh Kredit'; 'Grant Hanna'; 'Sean McCarthy'; 'Lisette Flores'; 'Brenden Foland'; 'Paulino Valerio'; 'Sean Laux'; 'SMONTENEGRO@azleg.gov'; 'Warren Petersen'; 'Oscar De Los Santos'; 'Priya Sundareshan'; Keely Varvel; Tonia Tunnell; Calli Jones  
**Subject:** Clarification of DHS/CISA Outreach and Federal Election Security Support  
**Attachments:** 2026 0205 - Follow-up Ltr. to Sec. Noem.pdf

Chairman Farnsworth and Members of the Joint Legislative Budget Committee,

Thank you for the questions raised during the January 29, 2026 JLBC meeting regarding the Secretary of State's engagement with DHS and CISA. We appreciate the opportunity to clarify the record.

**Prior outreach.** Secretary Fontes and his staff have engaged DHS and CISA for multiple years. Following the change in federal administration, Secretary Fontes sent a written letter to Secretary Noem on March 7, 2025 requesting confirmation that election security coordination and assistance would continue. That letter did not receive a response. After Arizona's June 2025 cyber incident, the Secretary's Office also sought assistance through Arizona's congressional delegation and through state partners, including the Arizona Department of Homeland Security and the Arizona National Guard.

**DHS/CISA responsiveness.** As discussed at the hearing, longstanding CISA points of contact were reassigned or no longer available, and staff indicated they were not equipped to provide the election security support previously relied upon. Aside from a general response letter to Congressman Stanton, our office received no specific guidance, recommendations, or pathway for continued federal assistance.

**Current follow-up.** On February 5, 2026, Secretary Fontes sent a formal follow-up letter to Secretary Noem seeking clarity on available election security services, the termination of MS-ISAC support, and any assistance for the 2026 election cycle. We are awaiting a response.

For additional context, we have attached an addendum summarizing recent bipartisan media reporting on changes at CISA and their impact on state and local election security support.

### **Addendum: Public Reporting on Changes at CISA and Election Security Support**

Over the past year, national media outlets have consistently reported bipartisan concern among election officials and election security experts regarding changes at the Cybersecurity and Infrastructure Security Agency (CISA) and the resulting reduction in support for states and counties. Coverage has documented CISA's withdrawal from election official conferences, confirmation that election security assistance to

states has been curtailed, and concerns that trust between CISA and election administrators has been significantly damaged.

[CISA cybersecurity agency skips conferences of state election officials - Votebeat](#)  
[CISA halts support for states on election security, U.S. official confirms - Votebeat](#)  
[Midterm worries as election security agency sees changes – NBC Los Angeles](#)  
[Election officials say trust with CISA is broken — and may not come back](#)

In June 2025, CISA released its FY 2026 budget proposal, which would eliminate its election security division entirely and reduce the agency’s workforce by approximately one-third. Members of Congress subsequently raised concerns about the operational impacts of those reductions.

[2026 budget proposal would axe one-third of CISA workforce - Defense OneLawmakers press acting CISA director on workforce reductions](#)

In October 2025, CISA terminated its agreement supporting the Multi-State Information Sharing and Analysis Center (MS-ISAC), which had provided cybersecurity tools and services to states and counties. No replacement funding or alternative support program has been announced.

[CISA kills agreement with nonprofit that runs MS-ISAC • The Register](#)

In January 2026, congressional budget staff indicated that election security funding might be restored in the CISA budget; however, no legislation has been enacted to date. As of January 2026, public reporting continues to describe significant staffing challenges within CISA.

[Congress Proposes Steep Cuts to CISA - GovInfoSecurity](#)  
[CISA Is 'Trying to Get Back on Its Mission' After Trump Cuts](#)  
[CISA’s 7 biggest challenges in 2026](#)



Greg Ensell  
*Chief Deputy Assistant Secretary of State  
and Deputy Chief of Staff*

Email: [Gensell@azsos.gov](mailto:Gensell@azsos.gov)  
Cell: (480) 244-5130  
Arizona Secretary of State | <https://azsos.gov>  
1700 W. Washington St., 7<sup>th</sup> Fl. | Phoenix, AZ 85007  
*This message and any messages in response to the sender of  
this message may be subject to a public records request.*



February 5, 2026

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

*Sent via email*

Dear Secretary Noem:

I write to follow up on my March 7, 2025, letter regarding the reduction in Department of Homeland Security support for election infrastructure security and the resulting risks to Arizona's election systems. To date, I have not received a response.

Since that correspondence, developments have further heightened my concern. Reporting from multiple nonpartisan and bipartisan sources indicates that state and local election officials nationwide continue to experience a significant erosion of coordination, technical assistance, and trust with the Cybersecurity and Infrastructure Security Agency (CISA). At the same time, DHS's FY 2026 budget proposal would eliminate CISA's election security functions entirely, and in October 2025 CISA terminated its agreement supporting the Multi-State Information Sharing and Analysis Center (MS-ISAC)—a core cybersecurity service relied upon by states and counties—with no replacement program in place.

Although Congress has restored some election security funding, no enacted legislation provides assurance that these capabilities will be reestablished, nor that experienced staff and operational capacity will be restored in time to support the 2026 election cycle. For Arizona and many other states, the practical effect remains the same: a diminished federal partnership at a time of sustained and well-documented foreign and domestic threats.

As outlined in my earlier letter, Arizona has faced cyber intrusions, foreign influence operations, bomb threats, and targeted intimidation of election officials. Historically, our ability to anticipate, deter, and respond to these threats has depended in part on timely federal intelligence sharing, cybersecurity tools, and incident-response coordination through DHS and CISA. The withdrawal of that support materially increases risk to election

1700 W. Washington St., FL 7  
Phoenix, AZ 85007-2808  
[www.azsos.gov](http://www.azsos.gov)

operations that are constitutionally administered by states but nationally significant in their consequences.

Given these developments, I respectfully request clarity on the following:

1. Whether DHS intends to restore or replace the election security services previously provided by CISA, including cybersecurity coordination and incident-response support for state and local election officials;
2. How DHS plans to address the gap created by the termination of MS-ISAC support; and
3. What assurances, if any, DHS can provide to states preparing for the 2026 election cycle that federal election security support will be stable, reliable, and operationally meaningful.

Absent clear answers, states will be forced to assume that federal election security assistance will remain limited or unavailable and to plan accordingly—often at significant cost and with unavoidable operational risk.

As my office continues to respond to a recent cyberattack, members of my state legislature have urged me to seek financial support from DHS and CISA, asserting that assistance remains available to other states. If that is accurate, I respectfully request that your office provide clear guidance on what assistance is currently available and how Arizona may formally access it.

Having received no response to my March letter—and based on direct communications with CISA staff following the change in DHS leadership, indicating that they were no longer equipped to provide assistance—my office coordinated our June 23, 2025 cyber incident response through the Arizona Department of Homeland Security and the Arizona National Guard. We also sought assistance through Arizona's congressional delegation, including Congressman Greg Stanton and U.S. Senators Ruben Gallego and Mark Kelly (see attached correspondence).

I understand that Arizona state legislators also contacted DHS and CISA following the incident. While your office reportedly stated to media outlets that DHS had been working with Arizona, I was never informed of any such response or provided with recommended follow-up actions. On July 21, 2025, *CyberScoop* reported the following statement from a DHS spokesperson:

“Here are the facts: In late June, the state requested assistance. On July 1st the Arizona Secretary of State posted a notice on their website and took their candidate portal offline for several days ahead of their primary special election. Since then CISA has been working with Arizona and has provided direct assistance to support their response efforts.”

Given my statutory responsibility for election administration—and the oversight role of state legislators responsible for funding ongoing remediation efforts—I need clarity regarding what assistance DHS and CISA did or did not provide and how states are expected to engage federal partners going forward.

Accordingly, I again urge DHS to renew its commitment to election security and to a transparent, reliable partnership with the states. Through this letter, I am formally requesting any federal funding or technical assistance that may be available to support the continued strengthening of Arizona’s election security posture.

My staff and I remain available to meet at your convenience to discuss these issues in greater detail. I appreciate your attention to this matter and look forward to your response.

Sincerely,



**Adrian P. Fontes**

Arizona Secretary of State



March 7, 2025

*Via Email*

Honorable Kristi Noem  
U.S. Department of Homeland Security  
Office of the Executive Secretary  
Mail Stop 0525  
Washington, DC 20528

Dear Secretary Noem:

As the Secretary of State of Arizona, I am writing to express grave concern for the ongoing reduction in vital security support of my state's, and the nation's, critical election infrastructure.

Secure election administration is the bedrock of American democracy, which makes it a prime target for physical and cyber threats against the United States. Information technology systems related to election administration are perennial targets of sophisticated cyber threat actors including nation-state and cybercriminal groups.

Since January 2017, the United States Department of Homeland Security (DHS) has designated election infrastructure as national critical infrastructure. I agree with this policy. While elections remain a state and local responsibility, this designation has allowed states to voluntarily partner with DHS and particularly with the Cybersecurity and Infrastructure Security Agency (CISA), utilizing cybersecurity and physical security services prioritized for state and local election offices. CISA's prioritized services help election agencies defend against these national security threats.

I understand you have completed your review of DHS's operations, priorities, and resource allocation, and that you do not plan to make your findings public. Related to this evaluation, CISA has completely ceased coordination with my office on election infrastructure security and support. What was until just last month a longstanding partnership on critical security matters is now complete radio silence from CISA staff except via one designee.

1700 West Washington, Seventh Floor  
Phoenix, Arizona 85007  
Telephone: (602) 542-8683  
Toll-free in Arizona 1-877-THE VOTE

This raises serious concerns for the security of Arizona's elections going forward. My state has faced numerous threats from both foreign<sup>1</sup> and domestic actors, including:

- A breach of the Arizona voter registration database by hackers linked initially to Russia, later to unknown cybercriminals, causing it to be shut down for nearly a week just prior to the voter registration cutoff for the 2016 election. Arizona was one of seven states that suffered attacks at that time.<sup>2</sup>
- Russian affiliated groups Storm-1516 and Foundation to Battle Injustice created AI-generated allegations that Arizona elected officials were orchestrating a plan to commit election fraud in the 2024 election in favor of specific candidates.<sup>3</sup>
- The intelligence community assesses that Russian influence actors recently posted and amplified an article falsely claiming that U.S. officials across swing states plan to orchestrate election fraud using a range of tactics, such as ballot stuffing and cyberattacks.<sup>4</sup>
- Bomb threats against polling centers in Arizona originating from Russian email domains during the 2024 election.<sup>5</sup>
- Threatening phone calls, emails, and letters against individual Arizona election officials, leading to difficulties in recruiting poll workers.<sup>6</sup>

Necessarily, these examples do *not* include any threats that may have been intercepted by DHS without becoming public knowledge, much less any prospective threats that were deterred by DHS's robust security operations support of our state infrastructure in the past.

My office's resources to anticipate and guard against threats to the integrity of Arizona's election system are limited. For us, DHS's withdrawal of the full cooperation and support of our partners at CISA means our capacity to conduct this important work will be severely compromised.

In light of these concerns, I am eager to discuss with you how DHS plans to address ongoing threats to the security of our election system. I ask for your continued commitment to leaving the services CISA provides to Arizona intact. These services are a key component of CISA's

---

<sup>1</sup> [https://www.cisa.gov/sites/default/files/2024-10/PSA\\_Just%20So%20You%20Know\\_Foreign\\_Threat\\_Actors\\_Likely\\_to\\_Use\\_a\\_Variety\\_of\\_Tactics.pdf](https://www.cisa.gov/sites/default/files/2024-10/PSA_Just%20So%20You%20Know_Foreign_Threat_Actors_Likely_to_Use_a_Variety_of_Tactics.pdf) (last visited March 6, 2025).

<sup>2</sup> <https://www.nbcnews.com/politics/elections/u-s-intel-russia-compromised-seven-states-prior-2016-election-n850296>; [https://www.washingtonpost.com/world/national-security/fbi-is-investigating-foreign-hacks-of-state-election-systems/2016/08/29/6e758ff4-6e00-11e6-8365-b19e428a975e\\_story.html](https://www.washingtonpost.com/world/national-security/fbi-is-investigating-foreign-hacks-of-state-election-systems/2016/08/29/6e758ff4-6e00-11e6-8365-b19e428a975e_story.html) (last visited March 6, 2025).

<sup>3</sup> <https://www.fbi.gov/news/press-releases/joint-odni-fbi-and-cisa-statement-110424> (last visited March 6, 2025).

<sup>4</sup> <https://www.ic3.gov/PSA/2024/PSA241018> (last visited March 6, 2025).

<sup>5</sup> <https://www.fbi.gov/news/press-releases/fbi-statement-on-bomb-threats-to-polling-locations>; <https://www.reuters.com/world/us/fake-bomb-threats-linked-russia-briefly-close-georgia-polling-locations-2024-11-05/> (last visited March 6, 2025).

<sup>6</sup> <https://www.reuters.com/world/us/kill-them-arizona-election-workers-face-midterm-threats-2022-11-06/>; <https://www.npr.org/2024/10/17/nx-s1-5154071/election-workers-in-arizona-are-facing-slurs-and-death-threats>; <https://www.justice.gov/archives/opa/pr/man-pleads-guilty-making-threats-arizona-election-office> (last visited March 6, 2025).

core mission which has provided great support in the past. My staff and I are available at your convenience to further explain why CISA is an essential partner in Arizona and our country, and look forward to your reply.

Sincerely,

A handwritten signature in green ink, appearing to read "Adrian P. Fontes". The signature is stylized with a large, looped initial "A" and a prominent "F".

ADRIAN P. FONTES  
Arizona Secretary of State

**GREG STANTON**  
ARIZONA'S FOURTH DISTRICT

**WASHINGTON OFFICE**  
207 CANNON BUILDING  
WASHINGTON, D.C. 20515  
(202) 225-9888

**DISTRICT OFFICE**  
1220 S. ALMA SCHOOL ROAD, STE. 209  
MESA, ARIZONA 85210  
(602) 956-2463

STANTON.HOUSE.GOV



**Congress of the United States**  
**House of Representatives**

**COMMITTEE ON TRANSPORTATION  
AND INFRASTRUCTURE**

**RANKING MEMBER**  
**ECONOMIC DEVELOPMENT, PUBLIC BUILDINGS, AND  
EMERGENCY MANAGEMENT SUBCOMMITTEE**  
AVIATION SUBCOMMITTEE  
HIGHWAYS AND TRANSIT SUBCOMMITTEE

**COMMITTEE ON FOREIGN AFFAIRS**  
WESTERN HEMISPHERE SUBCOMMITTEE

**SELECT COMMITTEE ON THE STRATEGIC  
COMPETITION BETWEEN THE UNITED STATES  
AND THE CHINESE COMMUNIST PARTY**

July 24, 2025

The Honorable Kristi Noem  
Secretary of Homeland Security  
U.S. Department of Homeland Security  
2707 Martin Luther King Jr. Ave SE  
Washington, DC 20528

Dr. Madhu Gottumukkala  
Acting Director and Deputy Director for CISA  
Cybersecurity and Infrastructure Security Agency  
1110 N. Glebe Road  
Arlington, VA 20598

Ryan Murray  
Chief Information Security Officer and Deputy Director  
Arizona Department of Homeland Security  
1802 W. Jackson Street, #117  
Phoenix, AZ 85007

Secretary Noem, Dr. Gottumukkala, and Mr. Murray:

We write to request a briefing on the June cyberattack on Arizona's state systems. We request this to be a Member-level briefing by August 15, 2025, to go over the contours of the attack, the efforts to secure Arizona's systems, and the cybersecurity coordination efforts between the federal and state governments across the country to keep our critical cybersecurity infrastructure secure.

Reporting indicates that the Iranian government or its affiliates are likely responsible for a cyberattack that breached Arizona's candidate web portal last month,<sup>1</sup> starting two days after the June 21 U.S. bombing of Iran. The hacker, who gained access to a server at the Arizona Secretary of State's office on June 23, changed candidate profile photos to a red and black image of Ayatollah Ruhollah Khomeini, the leader of the 1979 revolution that established Iran as an Islamic republic. The same IP address attempted to attack other, unnamed, Arizona agencies and other states.

---

<sup>1</sup> [12 News Arizona](#)

The United States is facing a more complex and dangerous security environment than ever before. A variety of foreign cybercriminals are targeting our advanced commercial capabilities, critical infrastructure, and economic well-being. At the same time, our federal cybersecurity agencies are facing cuts and downsizing – including at the Cybersecurity and Infrastructure Security Agency. This puts at risk our ability to quickly identify and stop attacks. We must build resilient systems that can protect against malicious attacks, including in Arizona.

Thank you in advance for your attention to this matter. We look forward to the briefing.

Sincerely,

A handwritten signature in black ink that reads "Greg Stanton". The signature is written in a cursive, flowing style.

---

Greg Stanton  
Member of Congress



U.S. Department of Homeland Security  
Cybersecurity & Infrastructure Security Agency  
Office of the Director  
Washington, DC 20528

September 5, 2025

The Honorable Greg Stanton  
U.S. House of Representatives  
Washington, DC 20515

Dear Representative Stanton:

Thank you for your July 24, 2025 letter regarding the recent cyber incident targeting Arizona's election systems. I appreciate your interest in the Cybersecurity and Infrastructure Security Agency's (CISA) efforts to assist the state of Arizona.

In late June, Arizona requested assistance from CISA, which was provided. On July 1<sup>st</sup>, the Arizona Secretary of State posted a public notice and took the candidate portal offline for several days ahead of their primary special election. Since then, CISA has been working with Arizona officials to support their response efforts.

The security of our Nation's election systems is paramount. Consistent with law, elections are administered by state and local governments. Under Secretary Noem's leadership, DHS and CISA are committed to ensuring that every state has the option to request cybersecurity and physical security assistance from the Department.

Thank you again for your letter. Should you wish to discuss this further, please do not hesitate to contact CISA's Office of Legislative Affairs at [CISA\\_OLA@mail.cisa.dhs.gov](mailto:CISA_OLA@mail.cisa.dhs.gov).

Sincerely,

A handwritten signature in black ink, appearing to read "M. Gottumukkala", written over a horizontal line.

Dr. Madhu Gottumukkala  
Acting Director

# 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.<sup>1</sup>

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.<sup>2</sup> 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

---

<sup>1</sup> *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/>.

<sup>2</sup> 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