

Head of US Cybersecurity Agency Sees Progress on Election Security, With More Work Needed for 2024

Efforts to protect the nation's election systems have grown exponentially since the 2016 presidential election, but more is needed to defend the integrity and resiliency of the election process ahead of next year's vote, the head of the nation's cybersecurity agency said Tuesday.

Jen Easterly, director of the U.S. Cybersecurity and Infrastructure Security Agency, known as CISA, announced plans to boost resources within the agency, hiring 10 additional election security specialists who will be across the country to interact directly with state and local officials. Easterly made the announcement at the summer conference of the National Association of State Election Directors in Charleston, South Carolina.

"Our capabilities and posture in this area is simply night and day when you compare it to 2016," Easterly told the officials gathered for her speech. "Despite this progress, we know there is more we have to do and that we must remain vigilant in the face of new and evolving risk."

CISA is charged with protecting critical infrastructure, including the nation's dams, banks and nuclear power plants. U.S. voting systems were added after the 2016 election and Russia's multipronged effort to meddle.

Since then, state and local election officials have been

working to shore up cybersecurity defenses around U.S. voting systems with the help of millions of dollars allocated by Congress over the years. In its efforts to secure elections, CISA works across government, partnering with federal, state and local agencies on various initiatives and providing direct support through cybersecurity reviews, assessments of physical security protocols, remote testing to look for vulnerabilities and other services.

Meanwhile, the threats to elections keep increasing, with the newest concern centered on the emergence of generative artificial intelligence tools that can be used by those seeking to meddle in U.S. elections to create false and misleading content. That's on top of financially motivated, criminal ransomware groups and the potential for sophisticated cyberattacks waged by countries hostile to the U.S.

Easterly, in an interview after her speech, said she was particularly concerned about the potential for bad actors to utilize generative AI, but expressed confidence that the public, with guidance from their state and local election officials, will be able to sort through manipulation attempts. She emphasized that the vote itself will be protected and secure.

Advertisement. Scroll to continue reading.

"All of the reasons why people should trust the integrity and security of elections remain the same: the physical security safeguards, the cybersecurity safeguards, all of the defense-in-depth mechanisms, the segmentation, the training that goes on," Easterly said. "Nothing will change all these safeguards and measures that are put in place to ensure the integrity and resilience of elections."

Since then, state and local election officials have been working to shore up cybersecurity defenses around U.S. voting systems with the help of millions of dollars allocated by Congress over the years. In its efforts to secure elections,

CISA works across government, partnering with federal, state and local agencies on various initiatives and providing direct support through cybersecurity reviews, assessments of physical security protocols, remote testing to look for vulnerabilities and other services.

Meanwhile, the threats to elections keep increasing, with the newest concern centered on the emergence of generative artificial intelligence tools that can be used by those seeking to meddle in U.S. elections to create false and misleading content. That's on top of financially motivated, criminal ransomware groups and the potential for sophisticated cyberattacks waged by countries hostile to the U.S.

Easterly, in an interview after her speech, said she was particularly concerned about the potential for bad actors to utilize generative AI, but expressed confidence that the public, with guidance from their state and local election officials, will be able to sort through manipulation attempts. She emphasized that the vote itself will be protected and secure.

"All of the reasons why people should trust the integrity and security of elections remain the same: the physical security safeguards, the cybersecurity safeguards, all of the defense-in-depth mechanisms, the segmentation, the training that goes on," Easterly said. "Nothing will change all these safeguards and measures that are put in place to ensure the integrity and resilience of elections."

After Easterly's speech, state election officials from Pennsylvania and Ohio said they welcomed the additional resources focused on election security and spoke about the importance of having good relationships with the federal government.

"The relationship needs to evolve and grow because our threat evolves and grows," said Mandi Grandjean, senior adviser and

deputy assistant to Ohio Secretary of State Frank LaRose, a Republican. “And the general landscape of what we do is evolving and growing. And so it’s great to hear what CISA is doing.”

<https://www.securityweek.com/head-of-us-cybersecurity-agency-sees-progress-on-election-security-with-more-work-needed-for-2024/>