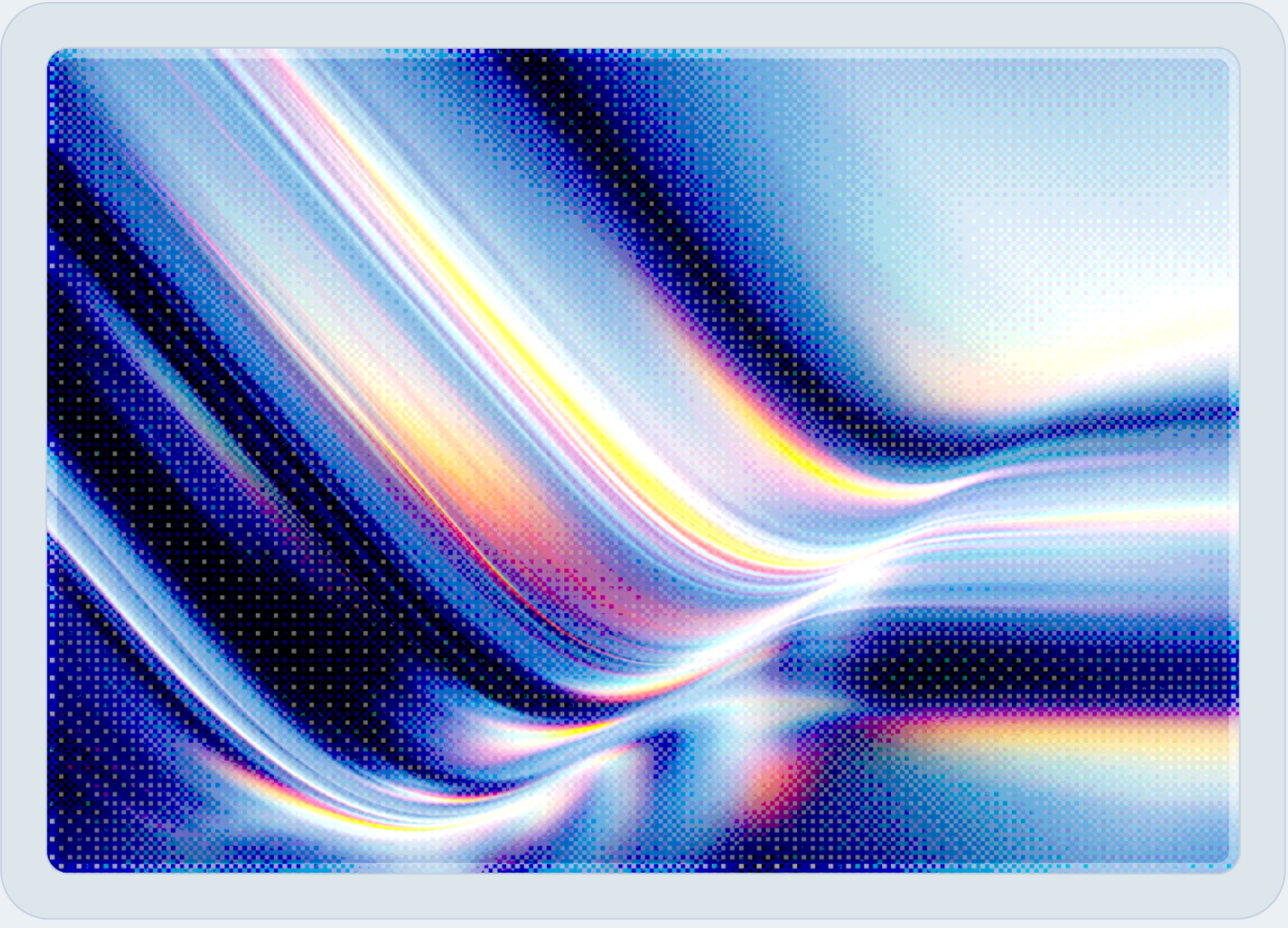
CSAI Foundation | Cloud Security Alliance

ONCD in Transition: US AI-Cyber Policy Continuity

Security Implications of the National Cyber Director's Exit for Enterprise and Critical Infrastructure Planning

2026-11-22

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

© 2026 Cloud Security Alliance. Some rights reserved.

You may download, store, display, view, print, redistribute, and link to this document in its original, unmodified form, provided that attribution to the Cloud Security Alliance is maintained and all trademark and copyright notices remain intact.

This document may not be modified or altered. You may quote portions of the document as permitted by the Fair Use provisions of the United States Copyright Act, provided that attribution is given to the Cloud Security Alliance.

This document may be shared on professional and social media platforms in its original form with attribution.

This document was generated with AI assistance and has not undergone official CSA review and approval processes.

Key Takeaways

Sean Cairncross's tenure as National Cyber Director ended on November 19, 2026, about fifteen months after he took office in August 2025. The White House confirmed his departure that day [1][2]. Accounts of how it came about differ. Axios, which first reported the exit, cited two sources who described it as amicable, while two White House officials said Chief of Staff Stephen Miller had pushed for the change [22]. Secondary coverage of that report said the timing was meant to leave room for a successor to be confirmed before Democrats take control of the Senate in January [23]. On November 20, President Trump told reporters that he had fired Cairncross because "I didn't think he was good enough" [4], and CyberScoop and CBS News also reported that he was fired [1][3].

Kirsten Davies, the Department of Defense's chief information officer, is taking over the Office of the National Cyber Director (ONCD). Outlets disagree on her exact status. CyberScoop and NBC News describe her role as acting, while CBS News and Axios report that the White House named her director, a post that requires Senate confirmation [1][2][3][22]. The exit comes at the end of a week of highly visible outages across cloud, aviation, banking, and national security networks, none of which has been linked to a common cause. It also comes as the White House is still implementing Executive Order 14409, which gives the National Cyber Director a consultative role in the major AI-cyber workstreams it creates [5][6].

Against this backdrop, CSA's assessment is that the leadership change is unlikely to alter the formal obligations already in force: the EO 14409 deadlines, CISA's binding directives, and the Gold Eagle clearinghouse. It does raise real continuity risk for work that depended on ONCD's coordinating role. That work includes the AI security policy framework ONCD announced in February 2026, the classified "covered frontier model" process, and implementation of the March 2026 national cyber strategy [7][8]. Since early October, the White House has also placed broader AI policy coordination in a task force led by the Director of National Intelligence, and Congress has since directed its AI-cyber concerns to that body rather than to ONCD [9][26]. That shift suggests the center of gravity for AI-cyber policy may move further away from ONCD while its leadership is in transition.

Security leaders do not need to change course. Because the policy direction will probably hold while its owners change, enterprises should anchor their programs to the instruments that are already in force rather than to statements by individual officials. They should also keep engaging the operational channels (CISA, the Gold Eagle clearinghouse, and their sector risk management agencies) that will outlast the transition, and treat the coming months as a period of lower federal policy clarity on AI-specific security expectations.

Background

ONCD's Mandate and Structural Limits

Congress created ONCD in 2021 to give the White House a Senate-confirmed official responsible for coordinating national cyber policy and strategy across the executive branch [6]. Cairncross was the office's third director, after Chris Inglis and Harry Coker. At his confirmation hearing he acknowledged that he lacked a "technical background in cyber" [6]. The office has always had limited formal authority. Writing in Lawfare in June 2026, Kevin Frazier quoted analysts who noted that the governing statute "confers the NCD with functions and responsibilities but few authorities independent of those already vested in the president," so the director's effectiveness depends largely on proximity to, and the confidence of, the president [6]. The same analysis observed that the administration's budget proposal would hold ONCD at 85 full-time employees while cutting its budget by $3 million [6].

These limits matter for continuity planning. ONCD does not run networks, issue binding directives, or regulate industry; CISA, OMB, the NSA, and sector agencies hold those levers [6]. ONCD's value lies in convening, prioritizing, and deconflicting. That value depends heavily on the personal standing of the director and on senior staff continuity. CyberScoop reported that the office had already been through turnover before Cairncross's exit. According to CyberScoop, his policy chief and senior adviser, Thomas Lind, left for OpenAI in October, and other senior staff departed after the AI executive order was issued [1].

The AI-Cyber Agenda Cairncross Leaves Behind

In 2026, ONCD placed itself at the junction of AI and cybersecurity policy. In February, Cairncross announced that the office was building an AI security policy framework, developed "hand-in-glove" with the Office of Science and Technology Policy, to "bolt security measures into U.S.-led AI tech stacks." No completion date was given [7]. In January, ONCD's principal deputy for policy described a diplomatic push to promote American AI cybersecurity standards and norms abroad [10]. On March 6, the administration released *President Trump's Cyber Strategy for America*, a short, deliberately high-level document organized around six pillars: shaping adversary behavior, promoting common-sense regulation, modernizing federal networks, securing critical infrastructure, sustaining superiority in critical and emerging technologies (largely AI), and building talent [8]. Officials said more detailed implementation guidance would follow [8].

The most consequential instrument was Executive Order 14409, "Promoting Advanced Artificial Intelligence Innovation and Security," signed June 2, 2026, and published in the Federal Register on June 5 [5]. An earlier draft had been pulled hours before a planned signing. According to Lawfare, citing Politico, Treasury Secretary Scott Bessent had pressed for action out of concern that Cairncross "was not moving swiftly enough" [6]. The final order is a scaled-back, explicitly voluntary instrument of under 1,200 words [11]. Cairncross later defended its non-regulatory design at Black Hat 2026, arguing that a regulatory regime "would be obsolete 48 hours after" it completed its process [12].

The November Outage Cluster

Between November 12 and November 17, 2026, Microsoft 365, Workday, the FAA's national airspace system, AWS us-east-1, JPMorgan Chase's interbank processing, United Airlines, Apple's services, and the NSA's classified internal network all experienced disruptions [13]. Every organization that published a cause pointed to an internal factor, such as a latent defect, a failover, a disaster-recovery test, or an internal update. On November 17, the Director of National Intelligence said there were no "indicia of a coordinated cyberattack" [13][14]. The DNI himself attributed the failures to patching and upgrade work [14], and some reporting linked the cluster to accelerated patching of AI-discovered vulnerabilities. CSA's prior analysis, however, found no public evidence that such patching caused any specific outage [13]. Coverage of Cairncross's exit tied its timing to the outages, though no outlet reported that they were the stated reason [2][3]. On November 17, Senators Maria Cantwell and Mike Rounds sent a bipartisan letter to DNI Jay Clayton, in his capacity as head of the White House AI task force, on AI-enabled cyber threats. The letter stated that "what is missing is a coordinated national strategy" [15][26], and the senators publicly urged the White House to take "immediate action" [28]. It followed an October 13 letter on the same subject addressed to both Clayton and OSTP Director Michael Kratsios [27].

Security Analysis

What Is Locked In Versus What Depends on ONCD

The most useful way to assess continuity risk is to separate obligations that already exist in law, executive order, or binding directive from work that still depends on ONCD's coordination. EO 14409 names the National Cyber Director in roughly half of its operative provisions, Sections 2(c), 2(d), 2(e), and 3, and in each case as a consulting or coordinating party rather than the lead [5]. The table below maps those provisions, together with the most recent public reporting on each one's status.

EO 14409 Provision	Lead Agency	ONCD Role	Last Publicly Reported Status	Continuity Exposure
Sec. 2(c): CISA Binding Operational Directives for civilian systems and expanded access to AI-enabled defensive tools	DHS/CISA	Consulted (with OMB and National Security Advisor)	BOD 26-04 issued June 10, 2026 [16]	Low; directive authority sits with CISA
Sec. 2(d): AI cybersecurity clearinghouse to coordinate vulnerability scanning, validation, and patch prioritization	Treasury	Consulted (with NSA and CISA)	Launched as Gold Eagle, July 14, 2026 [17][18]	Low to moderate; operational, but governance details remain unpublished
Sec. 2(e): Federal grant funding for AI vulnerability detection	OMB	Coordinating partner (with CISA)	No public determination identified as of November 2026	Moderate
Sec. 3(a): Classified benchmarking to designate "covered frontier models"	NSA determines, in consultation with NCD, OSTP, and CISA	Consultative, routed "through" the White House Chief of Staff	Framework finalized but unpublished (as of August 2026) [19]	Moderate; opaque process loses a civilian cyber voice
Sec. 3(b): Voluntary pre-release access (up to 30 days) and	Treasury, NSA, CISA	Consultative	In operation, criteria unpublished (as	Moderate

EO 14409 Provision	Lead Agency	ONCD Role	Last Publicly Reported Status	Continuity Exposure
trusted-partner selection			of August 2026) [19]	

The table points to a consistent pattern. The parts of EO 14409 that impose concrete requirements on federal agencies and shape enterprise patching behavior belong to agencies that are not affected by the ONCD transition. BOD 26-04, which CSA has analyzed as an emerging de facto patch baseline, remains in force regardless of who sits in the director's chair [16]. Gold Eagle is a Treasury-led operational program built on Carnegie Mellon SEI's VINCE platform, and it does not depend on ONCD leadership for its day-to-day function [18].

The work most exposed to the transition is the discretionary, policy-shaping work that ONCD was expected to drive. That includes the AI security policy framework, which has not been publicly released, as well as the detailed implementation guidance promised alongside the national cyber strategy and the international standards diplomacy [7][8][10]. Each of these depends on a director with the standing to convene agencies and to bargain with industry. Davies, whose most recent role has been as DoD CIO rather than in White House policy coordination [1][2], will likely need time to establish that standing, whether she serves in an acting capacity or as a nominee. The turnover among senior staff reduces the institutional memory available to compensate.

Leadership Gaps Are Compounding Across the Federal Cyber Apparatus

The ONCD transition does not happen in isolation. CISA has operated under an acting director, Nick Andersen, since late February 2026 [25]. The nominee to lead the agency, Michael LoSapio, faced what CyberScoop described as a contentious confirmation hearing on November 19, the same day Cairncross's exit was reported [1][24]. The two most prominent civilian cyber leadership posts in the federal government are therefore both in transition, with their occupants either serving in an acting capacity or awaiting Senate action. Meanwhile, the President named DNI Jay Clayton in early October to lead a new federal AI task force [9]. The Cantwell–Rounds letters on AI-enabled cyber threats went to Clayton in November and to Clayton and Kratsios in October, not to ONCD [26][27]. NBC's source described Davies as joining a team that includes Clayton, Kratsios, and Secretary of State and National Security Advisor Marco Rubio [2].

One structural detail of EO 14409 deserves attention. Section 3 routes the National Cyber Director's participation in frontier-model work "in consultation with the White House Chief of Staff, through the National Cyber Director" [5]. CBS News reports that Stephen Miller became chief of staff in early November and was the official who pressed for Cairncross's removal and selected his successor [3]. CyberScoop corroborates Miller's role as chief of staff [1], and Axios separately reported that White House officials said he pushed for the change [22]. If this reporting is accurate, these facts suggest that ONCD's voice in frontier-model designation now runs through a chief of staff who directly controls its leadership. That does not imply any change in policy direction. It does indicate that ONCD's independent influence over the most sensitive AI-cyber decisions may be smaller than its statutory role implies.

For enterprises, the practical consequence of this dispersion is ambiguity about who speaks authoritatively on AI-specific security expectations. Treasury leads the clearinghouse, NSA leads model benchmarking, CISA leads directives, the DNI leads the AI task force, and OSTP leads broader AI policy. ONCD was the logical integrator. With that integrator in transition, organizations should expect slower and less consistent signals, particularly on questions that span agencies, such as how covered-frontier-model designations should inform private-sector vendor risk decisions.

Signal Risk During the Transition

A transition of this kind creates two risks to how the federal government communicates about incidents. The first is the attribution problem CSA identified in the November outage cluster. Officials characterized the incidents as non-malicious before most root causes were published. Those characterizations were later consistent with vendor disclosures, but the sequence showed how quickly federal statements can run ahead of evidence, and how quickly speculation about AI involvement spread in the gap [13][14]. A cyber director's office in transition is less well placed to coordinate disciplined, evidence-based federal messaging during the next multi-sector incident. The second risk is policy whiplash. A new director, under pressure to show technical credibility and to answer the senators' call for a coordinated strategy, may announce new initiatives quickly. Those initiatives could overlap or conflict with the work Treasury, NSA, and CISA already have underway. Neither risk is certain, but both argue for organizations relying on binding instruments and operational channels rather than on announcements.

What Is Unlikely to Change

The administration's AI-cyber posture rests on a consistent set of commitments. They include voluntary rather than mandatory frontier-model review, AI-enabled defense, accelerated patching, and avoidance of new regulation, and they predate Cairncross and are written into EO 14409 itself [5][11]. Davies's public statement on taking the role emphasized dominating "the cyber landscape for generations to come,"

which, while general, gives no indication of a departure from that posture [2]. CSA therefore assesses that the substance of federal AI-cyber policy is likely to remain stable. The transition mainly affects pace, coordination quality, and the clarity of the signals enterprises receive.

Recommendations

Immediate Actions

Organizations should first confirm that their compliance and security roadmaps cite binding instruments rather than officials or speeches. Federal contractors and critical infrastructure operators should verify that their vulnerability management programs track CISA BOD 26-04 timelines and any follow-on directives, which do not depend on ONCD leadership. Teams that participate in, or plan to engage with, the Gold Eagle clearinghouse should confirm their points of contact at Treasury and CISA and should document their disclosure and remediation workflows, so that engagement continues without interruption if program governance is restructured.

Communications and incident response leaders should also review how they handle federal statements during multi-sector incidents. The November cluster showed that early official characterizations can precede root-cause evidence [13]. Incident playbooks should require root-cause evidence from vendors and service providers before an incident is classified as benign or malicious, whatever the public statements say.

Short-Term Mitigations

Over the next three to six months, organizations should treat federal AI-specific security guidance as provisional and build their programs on durable, framework-based controls. Mapping AI security governance to the CSA AI Controls Matrix (AICM) v1.1 gives organizations a stable baseline that remains valid whichever federal office eventually publishes the AI security policy framework. Organizations that consume frontier AI models should add questions to vendor due diligence about whether a supplier participates in the EO 14409 pre-release review process. They should also recognize that the designation criteria are classified and that participation cannot be independently verified [19].

Organizations should also give change velocity the attention it now requires. Whatever role accelerated patching did or did not play in the November outages, the pressure to remediate AI-discovered vulnerabilities quickly is real [13][26]. Staged rollouts, canary deployments, and rollback testing are the controls that keep accelerated patching from becoming a source of outages [13]. Policy and government-affairs teams should monitor the Senate's handling of a permanent National Cyber Director

nomination and the CISA director confirmation, since both will shape how quickly cross-agency guidance resumes. The reported aim of completing a confirmation before the change in Senate control in January makes the coming weeks especially relevant [23].

Strategic Considerations

Over the longer term, the ONCD transition highlights a structural question the security community should engage with directly: whether the National Cyber Director should hold stronger positional authority over AI-cyber coordination. Proposals in the policy literature include giving the director "lead responsibility" for emerging cyber risks and authority over cyber investments across the executive branch [6]. Industry associations and critical infrastructure sectors that rely on coherent federal coordination have an interest in contributing to that debate, including in response to the bipartisan congressional call for a coordinated national strategy on AI-enabled threats [26].

Organizations should also prepare for the possibility that AI-cyber policy coordination moves more permanently to the DNI-led AI task force or to Treasury. Such a shift would likely weight AI security policy more heavily toward national security and financial-sector framing. Enterprises in other sectors, such as healthcare, energy, and water, may need to be more proactive through their sector risk management agencies so that their operational realities are represented, particularly in the trusted-partner selection for early access to covered frontier models.

CSA Resource Alignment

CSA's most directly relevant prior work is its analysis of *Executive Order 14409: AI Cybersecurity Deadlines Take Effect* [20]. That note examined the order's 30-day and 60-day milestones and questioned how enforceable its voluntary framework would be. The current transition sharpens that concern: the order's discretionary elements, which ONCD was positioned to coordinate, are the elements most exposed to leadership change, while its directive-backed elements continue through CISA. Readers should use that analysis as the baseline map of which EO 14409 obligations apply to their organizations. CSA's *Trump's AI Cybersecurity Order: Voluntary Review, Enterprise Implications* [29] complements it with a closer look at the voluntary frontier-model review and the Treasury-led clearinghouse, the two mechanisms at the center of this note's continuity table.

CSA's research note *Gold Eagle: The White House's AI Vulnerability Clearinghouse* [18] covers the Treasury-led operational program that is the most concrete product of EO 14409 for critical infrastructure operators. It observed that the clearinghouse launched without published performance targets, dispute-resolution procedures, or data-protection details. Those gaps are less likely to be closed quickly while the

White House cyber coordination office is in transition. The companion note *EO 14409's Classified Frontier AI Framework: Opacity by Design* [19] covers the covered-frontier-model process in which ONCD's consultative role is now in question, along with its implications for vendor risk management.

The November Outage Cluster: Correlated Fragility and Attribution [13] gives the incident context for the departure. It is the basis for this note's recommendations on attribution discipline and change velocity. Finally, the CSA AI Controls Matrix (AICM) v1.1 [21] provides a vendor-neutral control baseline, including its governance, threat and vulnerability management, and supply chain domains. Organizations can anchor to it while federal AI security guidance is unsettled, so their programs do not depend on the timing of any single office's publications.

References

[1] Otto, Greg. "Sean Cairncross out as national cyber director." CyberScoop, November 19, 2026.

[2] Alba, Monica, and Kyla Guilfoil. "White House national cyber director is leaving the administration after series of tech outages." NBC News, November 19, 2026.

[3] Nicholson, Emma. "White House national cyber director leaving his post." CBS News, November 20, 2026.

[4] Combs, Cody. "Trump didn't think fired US cyber director Sean Cairncross was 'good enough'." The National, November 20, 2026.

[5] The White House. "Executive Order 14409: Promoting Advanced Artificial Intelligence Innovation and Security." Federal Register, Vol. 91, No. 108, June 5, 2026.

[6] Frazier, Kevin. "AI Cyber Risks Are Testing the Office Built to Coordinate Them." Lawfare, June 2, 2026.

[7] DiMolfetta, David. "White House cyber shop is crafting AI security policy framework, top official says." Nextgov/FCW, February 3, 2026.

[8] Starks, Tim. "The long-awaited Trump cyber strategy has arrived." CyberScoop, March 6, 2026.

[9] Associated Press. "Trump names National Intelligence Director Jay Clayton to lead a new federal AI task force." Associated Press via KY3, October 4, 2026.

[10] Starks, Tim. "US wants to push its view of AI cybersecurity standards to the rest of the world." CyberScoop, January 29, 2026.

[11] Johnson, Derek B. "Trump administration releases scaled-back AI executive order." CyberScoop, June 2, 2026.

[12] Starks, Tim. "National cyber director lays out White House plans to secure AI without writing new rules." CyberScoop, August 4, 2026.

[13] Cloud Security Alliance. "The November Outage Cluster: Correlated Fragility and Attribution." CSA AI Safety Initiative, November 18, 2026.

[14] Newsmax Wires. "DNI Dismisses Cyberattack Fears Amid Widespread Outages." Yahoo News, November 18, 2026.

[15] Strickler, Laura. "Amid string of outages, bipartisan letter urges strategy to combat AI-assisted cyber threats." NBC News via Yahoo News, November 18, 2026.

[16] Cloud Security Alliance. "From Executive Order to Enforcement: BOD 26-04's Patch Signal." CSA AI Safety Initiative, July 7, 2026.

[17] The White House. "White House Launches Gold Eagle Initiative for Unprecedented Cybersecurity Vulnerability Coordination." The White House, July 14, 2026.

[18] Cloud Security Alliance. "Gold Eagle: The White House's AI Vulnerability Clearinghouse." CSA AI Safety Initiative, July 16, 2026.

[19] Cloud Security Alliance. "EO 14409's Classified Frontier AI Framework: Opacity by Design." CSA AI Safety Initiative, August 12, 2026.

[20] Cloud Security Alliance. "Executive Order 14409: AI Cybersecurity Deadlines Take Effect." CSA AI Safety Initiative, July 6, 2026.

[21] Cloud Security Alliance. "AI Controls Matrix (AICM) v1.1." Cloud Security Alliance, 2025.

[22] Axios. "Scoop: Trump names Kirsten Davies as new national cyber director." Axios, November 19, 2026.

[23] AI Weekly. "Cairncross to Step Down as White House National Cyber Director." AI Weekly, November 2026.

[24] CyberScoop. "Dems call CISA nominee 'disqualified' after nomination hearing." CyberScoop, November 19, 2026.

[25] CyberScoop. "Gottumukkala out, Andersen in as acting CISA director." CyberScoop, February 2026.

[26] Cantwell, Maria, and Mike Rounds. "Letter to the White House Super Intelligence Task Force on AI and Cybersecurity." U.S. Senate Committee on Commerce, Science, and Transportation, November 17, 2026.

[27] Cantwell, Maria, and Mike Rounds. "Letter to DNI Jay Clayton and OSTP Director Michael Kratsios on AI and Cybersecurity." U.S. Senate Committee on Commerce, Science, and Transportation, October 13, 2026.

[28] Political Wire. "Senators Urge Immediate Action on AI Cyber Threats." Political Wire, November 18, 2026.

[29] Cloud Security Alliance. "Trump's AI Cybersecurity Order: Voluntary Review, Enterprise Implications." Cloud Security Alliance, 2026.