RISK BRIEFING, MIL/GOV & DEFENSE INDUSTRIAL BASE EDITION: A RUSSIAN CAMPAIGN NAMES YOUR SECTOR, TWO PATCH DEADLINES ALREADY PASSED, AND A COMPLIANCE WINDOW THAT REWARDS SHOWING UP

Date: 2026-07-28
From: The Stillwater Group in partnership with Datec
Classification: TLP:GREEN, shareable within your organization and with sector peers
Sector focus: Military, federal/state/local government, and defense industrial base organizations
Previous briefing: 2026-07-22 (26-09)

EXECUTIVE SUMMARY

A joint advisory sealed by 27 agencies across 16 countries this week put your sector at the top of a Russian espionage target list by name. AA26-204A, sealed July 23 by NSA, FBI, CISA, and Dutch intelligence plus 22 co-signers, documents Laundry Bear's year-long exploitation of Zimbra webmail and explicitly names the defense industrial base and federal and local government among the campaign's target sectors [6]. Proofpoint adds targeting of what it calls "nuclear installations" and "high science" [7]. The exploit executes when a victim views a phishing email, and a successful compromise yielded roughly 90 days of mailbox content, browser-stored passwords, two-factor backup codes, and session tokens: the raw material for contract intelligence, personnel targeting, and follow-on account takeover [6][8]. Even where large agencies and primes do not run Zimbra themselves, smaller suppliers, local governments, and university research partners may, so the hunt has to extend across your supplier base [6][8]. Meanwhile, two KEV-listed criticals carried a federal remediation deadline of July 25 that has already passed: a remote-code-execution flaw in on-premises Microsoft SharePoint (CVE-2026-50522) and an authentication bypass in Check Point Security Management (CVE-2026-16232), both platforms that government fleets run heavily [1]. For SharePoint, patching alone leaves attackers a way back in through stolen IIS machine keys, so key rotation and compromise hunting must follow [2]. On the policy front, three clocks are running: CMMC reform RFI comments are due at noon ET August 14, with obligations under DFARS 252.204-7012 fully in force in the meantime [48][49][50]; the CISA 2015 threat-sharing law sunsets September 30 unless the Senate acts, which would strip the liability shield under ISAC-style sharing [47]; and the AI Kill Switch Act (H.R. 9917) plus FedRAMP's patch-velocity ultimatum signal where federal software and AI procurement is heading [19][20][23]. With the election-year run-up underway, we have also made election infrastructure a standing topic below. Patch and hunt first; then work the compliance calendar, because this is a rare window where the DIB gets to shape its own rules.

SUMMARY OF IMMEDIATE ACTIONS

Priority	Action	Why Now
1	Confirm Zimbra is patched (CVE-2025-66376; current release 10.1.20) and hunt webmail for compromise going back a year; put the same question to suppliers, local-government partners, and university research collaborators	AA26-204A names the DIB and federal/ local government as Laundry Bear targets; the exploit triggers on viewing an email [6] [7][8]
2	Patch on-prem SharePoint (CVE-2026-50522), rotate ASP.NET/IIS machine keys, and hunt for webshells and forged-token persistence; federal agencies verify KEV compliance now, the July 25 deadline has passed	Mass exploitation began within hours of a July 20 public exploit; stolen machine keys survive patching [1][2][3]
3	Patch Check Point Security Management (CVE-2026-16232), pull management interfaces off the internet, and audit recent policy changes and admin activity	Actively exploited zero-day grants unauthenticated full admin over the firewall management server; same passed KEV deadline [1][4][5]
4	Apply the July 22 update to AA26-097A: inventory internet-reachable PLCs across agency and installation facilities systems and run the new project-file detection guidance	Iranian-affiliated actors are manipulating Rockwell, Schneider Electric, and Siemens PLCs at US water, energy, and government-services victims [13]
5	DIB contractors: file CMMC reform RFI comments by 12:00 pm ET August 14 and follow the July 30 SBA roundtable; keep 800-171 self-assessments, SPRS scores, and affirmations current	The comment window is open, and DFARS 252.204-7012 obligations remain binding with False Claims Act exposure attached [48][49][50]
6	Review with counsel what your threat-sharing participation looks like if CISA 2015 lapses September 30	The House provision passed 216-212 inside the NDAA; the Senate has no counterpart, and the liability shield lapses with the law [47]
7	Election offices and their vendors: verify election-sector information-sharing memberships and peer intel channels are active, harden voter-roll systems with MFA and anomaly detection, and schedule an AI-enabled disinformation tabletop	Threat-sharing legal protections are at risk on September 30, and Congress is already war-gaming AI-enabled infrastructure attacks [47][53]

Priority	Action	Why Now
8	Enforce travel-device discipline for cleared and senior personnel: dedicated travel devices, minimal local data, no stored credentials, full-tunnel VPN before anything else on hotel Wi-Fi	Manual border phone searches now require no suspicion in the Fourth Circuit, and hotel Wi-Fi gateways are being hijacked to serve MFA-bypassing fake Microsoft 365 logins [39][40][11]
9	Restrict outbound DNS to sanctioned resolvers and alert on high-volume or high-entropy queries	Malware is tunneling command-and-control through DNS, and hijacked gateways forge answers before they reach trusted resolvers [11][12]
10	Vendors selling software or AI into government: put your critical-vulnerability remediation clock in writing against FedRAMP 20x's two-to-four-day expectation, and track H.R. 9917's shutdown and incident-reporting provisions	The FedRAMP director says slow-to-patch vendors should exit the federal market; the kill-switch bill signals where AI procurement terms are heading [23][19][20]

WHAT'S CHANGED SINCE JULY 22

- **The Zimbra espionage campaign got its advisory, and it names this sector.** Joint advisory AA26-204A (July 23) formally documents Laundry Bear's exploitation of Zimbra CVE-2025-66376, with the defense industrial base and federal and local government among the named target sectors [6].
- **Two new KEV-listed criticals, and the federal clock already ran out.** CISA added SharePoint CVE-2026-50522 and Check Point CVE-2026-16232 to the Known Exploited Vulnerabilities catalog on July 22 with a July 25 federal remediation deadline [1].
- **CMMC reform now has hard dates.** An SBA Advocacy roundtable is set for July 30 and RFI comments are due at noon ET August 14 [48][49].
- **CISA 2015 reauthorization advanced one chamber.** The House passed its FY2027 NDAA (216-212) with a provision extending the threat-sharing law through 2036; the Senate has no matching provision and the September 30 sunset still stands [47].
- **The AI incident produced legislation.** H.R. 9917, the AI Kill Switch Act, was introduced July 23 with bipartisan sponsorship [19][20].
- **The Iranian PLC advisory expanded.** The July 22 update to AA26-097A adds Schneider Electric and Siemens equipment to the previously Rockwell-focused guidance, ships new detection content, and lists government-services facilities among the victims [13].

- **Holding steady:** wp2shell and FortiBleed remediation guidance is unchanged; nginx CVE-2026-42533 still has no public exploit, though a proof-of-concept has been announced for ~August 5 [9][10].

LAUNDRY BEAR: THE ESPIONAGE CAMPAIGN THAT NAMES YOU

- **What the advisory says.** AA26-204A (July 23) documents a Russian state-linked actor, tracked as Laundry Bear, Void Blizzard, and TA488, exploiting a cross-site-scripting flaw in Zimbra webmail (CVE-2025-66376, patched November 2025, exploited as a zero-day before that) through a view-based exploit delivered by phishing email: opening or previewing the message is enough, with no attachment or link click required [6]. The advisory's named target sectors read like this briefing's distribution list: the defense industrial base, federal and local government, education, energy, law enforcement, media, NGOs, and technology [6]. Proofpoint, which coined the "half-click" label, additionally reports targeting of what it calls "nuclear installations" and "high science" [7].
- **What a compromise costs.** A successful intrusion yielded roughly 90 days of mailbox content, browser-stored passwords, two-factor backup codes, and session tokens [8]. For this sector, that is contract correspondence, program contact directories, and the credentials to impersonate the people in them. Ninety days of a contracts officer's or program manager's mailbox is a targeting package.
- **Where to hunt.** Zimbra deployments often sit where large agencies and primes have least visibility: small suppliers, municipal and county governments, and university research partners. If you run it, patch and upgrade (10.1.20 shipped July 20 with nine additional critical fixes) and hunt for historical compromise going back a year [8]. If you do not run it, ask who in your supply chain and research-collaboration base does, because their compromised mailbox carries your program information and their hijacked identity is the phishing lure your staff will trust [6][8].
- **Enforcement is engaged.** An alleged group member was extradited from Thailand and is facing charges in Boston federal court, a signal that this campaign has sustained law-enforcement attention and that indicators and reporting channels are active [8].
- **Related activity worth one line each.** CERT-UA warns that UAC-0099 is delivering its MATCHBOIL.V2 loader through a counterfeit Notepad++ plugin against Ukrainian targets; organizations with Ukraine-facing operations or partners should fold the indicators into monitoring [51]. A Daily NK report, resting on a single anonymous source and explicitly unverified, describes North Korea arresting former military hackers for allegedly stealing from the regime's own banks; treat it as unconfirmed color, while the well-sourced context (a record $2 billion in DPRK crypto theft last year per Chainalysis) remains the durable planning fact [55].

PATCH NOW: TWO KEV EMERGENCIES, FEDERAL DEADLINE PASSED

- **Microsoft SharePoint CVE-2026-50522 (CVSS 9.8, on-premises only).** A deserialization flaw in SharePoint Subscription Edition, 2019, and 2016 allows remote code execution; SharePoint Online is unaffected [3]. Microsoft patched it July 14; a public exploit landed July 20 and mass exploitation followed within hours [2]. On-premises SharePoint remains a workhorse for agency intranets and contractor program collaboration, which often means CUI sits on these servers. The detail that matters most: watchTowr reports attackers using a single request to steal IIS machine keys, which let them forge valid authentication tokens and walk back in after you patch [2]. CISA's hardening guidance is blunt: assume compromise on internet-exposed unpatched servers, hunt and remediate, then rotate machine keys [1][2]. Federal agencies were required to remediate by July 25 under the KEV directive; verify your compliance evidence now rather than during the audit [1].
- **Check Point Security Management CVE-2026-16232 (CVSS 9.1).** An improper-authentication flaw lets an unauthenticated attacker obtain a token and authenticate with full administrative rights over the Security Management Server, which means the ability to rewrite firewall policy for everything the platform manages [4][5]. Check Point confirms in-the-wild exploitation against "a very small number of customers" and has shipped fixes (R81.20 JHF T158+, R82 T118+, R82.10 T36+) [4]. Where government and defense networks run Check Point management; treat any confirmed compromise as a potential full-network exposure event, audit recent policy changes and administrator activity, and get management interfaces off the open internet. The same July 25 federal deadline applied [1].
- **Patch-status watchlist.** wp2shell exploitation of WordPress continues at internet scale, and compromised sites serve fake Microsoft 365 and banking overlays to visitors, so exposure extends to public-affairs and recruiting sites and to the staff who browse them [10]. nginx CVE-2026-42533 remains unexploited in public, but a researcher-announced proof-of-concept is expected around August 5; close out patch verification first [9]. FortiBleed guidance is unchanged: credential rotation, session termination, and MFA remain the only complete fix.

COMPLIANCE AND POLICY: THREE CLOCKS RUNNING

- **A new export-control surface for nuclear-adjacent contractors.** On July 22 the United States and Saudi Arabia announced a Section 123 civil-nuclear cooperation agreement with a bilateral safeguards arrangement, now submitted to Congress for review and therefore not in force [59]. Contractors, laboratories, and engineering firms that expect to participate should begin export-authorization and information-protection reviews early rather than at contract award, and should assume a partnership of this profile draws state-sponsored collection against the firms inside it.
- **CMMC reform: work the window, keep the controls.** The Phase 2 suspension continues, and the reform process now has actionable dates: an SBA Advocacy small-business roundtable July 30 and RFI

comments due at 12:00 pm ET on August 14 [48][49]. Every legal analysis published this week agrees on the operative point: DFARS 252.204-7012, NIST 800-171 self-assessments, SPRS scores, and annual affirmations remain binding, with False Claims Act exposure attached [50]. Do not stand down a compliance program because certification enforcement paused; a stale SPRS score or an inaccurate affirmation is still an FCA problem today. Use the pause to close POA&M items, and use the RFI to put your assessment-cost and timeline experience on the record, because this is the mechanism through which the rules get rewritten [48][49][50].

- **CISA 2015 sunset: contingency time.** The House passed its FY2027 NDAA (216-212) with a provision reauthorizing the Cybersecurity Information Sharing Act of 2015 through 2036; the Senate draft has no counterpart provision and floor opposition exists, so the September 30 sunset remains live [47]. The liability, antitrust, and FOIA protections that underpin ISAC-style sharing lapse if nothing passes. For agencies and contractors whose intel picture depends on DIB-wide and sector indicator exchange, the action is a counsel review now: which of your sharing relationships rest on the statute's protections, and what does participation look like without them [47].
- **H.R. 9917 and the FedRAMP signal: where procurement is heading.** The AI Kill Switch Act, introduced July 23 with bipartisan sponsorship, would require AI developers above defined thresholds ($100 million in training compute or $500 million in revenue) to maintain shutdown capability, report qualifying incidents within 15 days, and comply with graduated federal correction orders issued through DHS with Commerce and DNI involvement; civil penalties scale to $20 million per day [19][20]. It is one chamber's freshly introduced bill, but paired with FedRAMP director Pete Waterman's statement that vendors who cannot patch critical internet-facing flaws inside FedRAMP 20x's two-to-four-day expectations should exit the federal market, the direction is clear: patch velocity, incident-reporting clocks, and AI shutdown capability are becoming procurement terms [19][23]. If you sell software or AI into government, get your answers in writing before a contracting officer asks; if you buy, borrow the standard in your own solicitations [23].
- **Post-incident lessons for agency AI programs.** Analysis of the Hugging Face incident has converged on a point that maps directly onto agency and contractor AI pilots: model-level safeguards are not a security boundary, and effective controls live outside the model in network rules, scoped credentials, destination allow lists, and outbound data-loss prevention [22]. Two governance wrinkles deserve contract language: Hugging Face says commercial frontier-model APIs refused to analyze attack artifacts during incident response, forcing a fallback to a self-hosted model, and a single-outlet, so-far-unconfirmed claim alleges OpenAI took roughly ten days to notify Hugging Face [21][22][58]. Put AI incident-notification clocks in vendor contracts and pre-approve a forensic-model plan so guardrails cannot lock responders out mid-incident [21][22].

ELECTION SECURITY (STANDING TOPIC)

With the election-year run-up underway, this section will appear in each Mil/Gov edition through the cycle. It is operational and strictly apolitical: the concern is the availability and integrity of election infrastructure and the intelligence channels that defend it, whoever wins.

- **The threat-sharing channel itself is at risk.** Election offices lean harder than almost any other government function on shared indicators, because most offices are small and depend on collective defense. The legal protections that underpin that sharing lapse September 30 if the CISA 2015 reauthorization stalls; the House provision passed 216-212 and the Senate has no counterpart [47]. State and local election offices, and the vendors who serve them, should verify now that each election-sector information-sharing membership you hold is current, that peer intelligence channels have named owners, and that counsel has reviewed what indicator sharing looks like without the statute's liability shield [47].
- **AI-enabled scenarios are already on Congress's tabletop. Put them on yours.** Members of two House committees ran a first-of-its-kind closed-door exercise simulating AI-enabled cyberattacks against US ports, rail, and airports in a 2027 Taiwan-crisis scenario [53]. The exercise format transfers directly: election offices and their vendors should tabletop AI-enabled disinformation targeting voter confidence alongside infrastructure scenarios such as voter-roll manipulation or registration-system outage during a registration deadline [53].
- **Harden the systems that hold the rolls.** The controls regulators and settlements keep pricing elsewhere in this briefing apply squarely to voter-registration systems: MFA on every administrative account, rate limiting, and login-anomaly detection, plus documented recovery for registration data [31][47]. Small offices should route hardening requests through their sector information-sharing and state channels rather than waiting for an incident to surface the gap [47].

OPERATIONAL TECHNOLOGY, FACILITIES, AND THE SUPPLY CHAIN

- **Iranian-affiliated actors are on government-services facilities.** The July 22 update to joint advisory AA26-097A (CISA, FBI, NSA, and DOE) confirms that Iranian-affiliated actors manipulating internet-exposed PLCs at US water, energy, and government-services victims since at least March are now observed on Schneider Electric and Siemens equipment in addition to Rockwell [13]. The actors exfiltrate PLC project files, alter or delete control logic, manipulate operator displays, and in at least one FBI-observed case installed a malicious project file that preserved normal downstream function while overriding safe-operating parameters [13]. Agency and installation facilities teams should treat themselves as named in this advisory: building automation, water treatment, and power systems on bases and campuses run the same controllers. Inventory anything internet-reachable, pull it behind secure gateways, and run the advisory's new project-file detection guidance [13].

- **Supplier custody of facility design data: the Kudankulam lesson.** In mid-July, the World Leaks extortion group published roughly 19,000 files (14.3 GB) taken from India's Reliance Group via a third-party-hosted server, purportedly including ventilation and cooling blueprints and a control-room floor layout for two under-construction units at the Kudankulam nuclear plant; the operator says the material involves only conventional common-service facilities, and authenticity is unverified [18]. The failure mode is the point for this audience: facility design data left the owner's control through an engineering contractor's outsourced hosting, and the extortionists priced the criticality of the end client rather than the breached party. Contractor-held CUI fails the same way. Map where program drawings, facility layouts, and technical baselines sit in subcontractors' and their hosting providers' hands, and put custody terms in the flow-down [18].
- **Aviation cyber governance, graded.** GAO's new report (GAO-26-107693) finds the FAA has defined cyber roles while TSA has not, and that TSA's cyber roadmap dates to 2018 and is misaligned with DHS strategy; both departments agreed with all five recommendations [52]. Worth quoting precisely in your own briefings: GAO reports there have been no reports of successful cyberattacks on avionics, so the demonstrated risk concentrates in ground systems and governance, and vendor claims otherwise are ahead of the evidence [52]. For military and government aviation stakeholders, the report is a ready-made template for asking the same roles-and-roadmap questions internally.
- **Third-party exposure keeps arriving through business systems.** Coca-Cola told regulators a ransomware attack forced it to suspend US production at its fairlife subsidiary, a reminder that production stops when IT stops, without any OT compromise [14][15]. Ernst & Young notified clients that tax and financial documents were exposed through a third-party IT support-ticket platform, and former Nissan employees are suing over HR data stolen from a hosted PeopleSoft system; in both patterns, the customer of the breached platform absorbs the consequence, and for a contractor that consequence can include CUI scoped into a helpdesk ticket or cleared-workforce PII in a hosted HR stack [35][30]. The 23andMe multistate settlement adds an M&A note: its security obligations survived bankruptcy and bind the buyer, which DIB acquirers consolidating smaller suppliers should read as a due-diligence instruction [31][32].
- **Manufacturing telemetry, for DIB producers.** SonicWall's manufacturing brief reports sector intrusion-prevention events down 56.2% year over year yet still totaling 474 million in the first half of 2026, with attacks shifting toward IoT and SCADA entry points; the figures are one vendor's telemetry skewed toward smaller networks, which describes much of the lower-tier DIB [54].

COUNTER-SURVEILLANCE: YOUR PEOPLE, YOUR DEVICES, AND YOUR TRAVEL

The Laundry Bear advisory above is the loud version of a quieter theme running through this week: collection aimed at people rather than infrastructure. A mailbox, a phone at a border crossing, and a laptop on a conference network are all routes to the same thing, which is knowing who your people are, who they work with, and where they will be. For a cleared workforce that matters even when nothing classified moves, because the pattern itself is the intelligence. Handle the following as one travel-and-personnel programme.

- **The border search threshold dropped.** In U.S. v. Belmonte Cardozo (decided July 13), the Fourth Circuit held that manual, hand-operated phone searches at the border require no warrant and no individualized suspicion; forensic searches still require some measure of individualized suspicion under existing circuit precedent [39][40]. The published opinion binds Maryland, the Carolinas, Virginia, and West Virginia, home to a large share of this sector's workforce. For cleared and senior personnel crossing borders, the control is data minimization: dedicated travel devices, minimal local data, and no stored credentials, because the legal threshold protecting a device at the border keeps dropping [39][40].
- **Hotel Wi-Fi is a credential trap.** ReliaQuest reports an ongoing campaign, active since at least June, in which attackers alter DNS settings on hotel and conference-center Wi-Fi gateways so travelers land on convincing fake Microsoft 365 portals; in some cases a device-code sign-in flow captured a legitimate OAuth session and bypassed MFA outright [11]. Conference season puts program staff on exactly these networks. The fix is architectural: full-tunnel VPN before anything else on untrusted networks, encrypted DNS in strict mode, and disabling the Entra device-code flow where the business does not need it [11]. Pair that with DNS egress control at home station, because Fortinet's documentation of a backdoor running command-and-control entirely over DNS shows what an uninspected resolver path is worth to an adversary [12].
- **Extortion mail will cite real data.** A mass sextortion campaign is demanding $2,000 in Bitcoin using genuinely leaked breach data to look credible, with no actual device compromise behind the claims [37]. A cleared workforce is a high-value audience for this pressure; pre-position plain-language guidance so employees report the mail through security channels instead of paying or hiding it [37].
- **Briefly noted.** Agencies procuring drone-as-first-responder systems should note that widely recirculated Flock Alpha performance figures are the vendor's own claims from an October 2025 launch, and that civil-liberties litigation pressure on surveillance-tool retention is rising, so verify performance and retention posture independently before award [43][41]. OpenAI's new Health in ChatGPT feature is a workforce-policy question: acceptable-use guidance should address employees connecting regulated-class personal data to consumer AI apps [27][28]. Airbus's migration of critical applications to a French trusted-cloud provider signals that data-residency and sovereignty terms are spreading through allied-nation procurement, and US firms serving European defense customers should expect the questions in RFPs [56][57].

What to do: make travel a controlled activity. Clean travel devices with minimum data, no stored credentials, no cached mailbox. Full-tunnel VPN before any other traffic on an untrusted network, and disable the Entra device-code sign-in flow where it is not operationally required. Brief travelers explicitly that a manual phone search at the border now requires no suspicion in the Fourth Circuit, and that the protection they may assume exists no longer does. Rotate credentials used on the road when people return rather than treating a quiet trip as a clean one. Where personnel hold clearances or program knowledge, apply this to conference attendance and site visits as well, not only international travel.

THE AI AGENT ATTACK SURFACE, BRIEFLY

- Manifold Security reports that any malicious co-installed browser extension can hijack Claude for Chrome's agent actions via synthetic clicks, reproducible in the current release as of late July despite a May report; machines running AI browser agents need enterprise extension allow-listing, and agencies piloting agents should treat this as a deployment gate [24]. Tego AI published a disputed Claude Code behavior in which a repository-committed instruction file can expose one out-of-project file; Anthropic closed the report as consistent with its documented threat model, so treat it as a boundary dispute and treat repository trust prompts as code-execution consent, a policy worth writing down for development teams handling CUI-adjacent code [25]. Varonis's "Dolphin X" stealer, advertising an AI-based victim-ranking profiler, is mostly seller-advertised capability so far, but the direction (automated triage of thousands of infections to find the valuable ones) raises the stakes of any single infected developer endpoint [26].

WHAT YOU SHOULD BE DOING RIGHT NOW

Immediate Actions (This Week)

1. **Verify Zimbra patching** (CVE-2025-66376; current release 10.1.20) and hunt for historical webmail compromise going back a year; send the same question to suppliers, local-government partners, and university research collaborators, and track their answers [6][7][8].
2. **Patch on-premises SharePoint** (Subscription Edition, 2019, 2016) for CVE-2026-50522, then rotate ASP.NET/IIS machine keys and hunt for webshells and forged-token persistence; assume compromise on servers that sat exposed and unpatched after July 20, and confirm KEV-deadline compliance evidence [1][2][3].
3. **Patch Check Point Security Management** for CVE-2026-16232, take management interfaces off the internet, and audit recent policy changes and admin logins for tampering [1][4][5].
4. **Act on AA26-097A's July 22 update** across agency and installation facilities: inventory internet-reachable PLCs on Rockwell, Schneider Electric, and Siemens estates, pull them behind secure gateways, and run the advisory's project-file detection guidance [13].

5. **Harden traveling and cleared staff**: dedicated travel devices with minimal data and no stored credentials for border crossings, always-on full-tunnel VPN, strict encrypted DNS, and disabled Entra device-code flow where unneeded [39][40][11].
6. **Close the DNS egress blind spot**: restrict workstation DNS to sanctioned resolvers and alert on high-volume or high-entropy DNS to unfamiliar domains [11][12].
7. **Election offices and vendors**: confirm sector information-sharing memberships and peer channels are live, verify MFA and login-anomaly detection on voter-roll and registration systems, and calendar an AI-enabled disinformation and infrastructure tabletop [47][53].
8. **Confirm wp2shell and nginx patch completion** before the announced ~August 5 nginx proof-of-concept [9][10].
9. **Pre-position scam-response guidance** for extortion mail citing real breach data, aimed at getting cleared employees to report rather than pay or conceal [37].

Strategic Actions (This Month)

1. **Work the CMMC reform window**: attend or follow the July 30 SBA roundtable, file RFI comments by noon ET August 14 with your real assessment-cost data, and keep 800-171, SPRS, and affirmation posture current in the meantime, because FCA exposure did not pause [48][49][50].
2. **Run the CISA 2015 contingency review with counsel**: inventory which sharing relationships rest on the statute's liability, antitrust, and FOIA protections and decide your posture if September 30 arrives without reauthorization [47].
3. **Map supplier custody of design and facility data**: the Kudankulam leak traveled through a contractor's outsourced data center and the EY exposure through an IT-support SaaS; find where your drawings, layouts, and technical baselines sit in other people's clouds and fix the flow-down terms [18][35].
4. **Put patch-velocity and AI terms into procurement on both sides**: if you sell to government, document your critical-vulnerability clock against FedRAMP 20x's two-to-four-day standard and track H.R. 9917; if you buy, write the same clocks and AI incident-notification terms into your solicitations [23][19][20].
5. **Pre-approve a forensic-AI plan** (self-hosted or contractually guaranteed) so a provider's guardrails cannot stall incident response, and add AI shutdown-and-notification questions to vendor governance reviews [21][22].
6. **Gate AI browser agents and coding assistants**: enterprise extension allow-listing on any machine running an agent, no autonomous modes on CUI-adjacent work, and repository trust prompts treated as code-execution consent [24][25].
7. **Use GAO-26-107693 as an internal template**: ask your own aviation, logistics, and facilities programs the same roles-defined and roadmap-current questions GAO asked FAA and TSA [52].

REFERENCES

[1] CISA Adds Two Known Exploited Vulnerabilities to Catalog (July 22, 2026) — https://www.cisa.gov/news-events/alerts/2026/07/22/cisa-adds-two-known-exploited-vulnerabilities-catalog

[2] SharePoint CVE-2026-50522 Exploited After Public PoC; Machine-Key Theft Defeats Patch-Only Response (July 22, 2026) — https://www.helpnetsecurity.com/2026/07/22/sharepoint-cve-2026-50522-exploited/

[3] Microsoft Security Update Guide: CVE-2026-50522 (July 14, 2026) — https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50522

[4] Check Point Support Advisory sk185169: CVE-2026-16232 (July 2026) — https://support.checkpoint.com/results/sk/sk185169

[5] Rapid7 Emergent Threat Response: CVE-2026-16232 Check Point SmartConsole Authentication Bypass Exploited in the Wild (July 23, 2026) — https://www.rapid7.com/blog/post/etr-cve-2026-16232-critical-check-point-smartconsole-authentication-bypass-exploited-in-the-wild/

[6] CISA/NSA/FBI/AIVD/MIVD Joint Cybersecurity Advisory AA26-204A: LAUNDRY BEAR Exploitation of Zimbra Collaboration (July 23, 2026) — https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-204a

[7] Proofpoint: TA488 Targets Zimbra Mailservers With Half-Click Exploits (July 23, 2026) — https://www.proofpoint.com/us/blog/threat-insight/ta488-targets-zimbra-mailservers-half-click-exploits

[8] Russian Espionage Hackers Hit Zimbra With Half-Click Attacks (July 24, 2026) — https://www.healthcareinfosecurity.com/russian-espionage-hackers-hit-zimbra-half-click-attacks-a-32322

[9] Critical NGINX Vulnerability Can Crash Workers and May Allow Remote Code Execution (July 19, 2026) — https://thehackernews.com/2026/07/critical-nginx-vulnerability-can-crash.html

[10] What Happens If You Visit a WordPress Site Hacked Through wp2shell (July 21, 2026) — https://www.malwarebytes.com/blog/bugs/2026/07/what-happens-if-you-visit-a-wordpress-site-hacked-through-wp2shell

[11] Hackers Hijack Hotel Wi-Fi DNS to Steal Microsoft 365 Accounts (July 24, 2026) — https://www.bleepingcomputer.com/news/security/hackers-hijack-hotel-wi-fi-dns-to-steal-microsoft-365-accounts/

[12] New TrickBot Variant Spotted Using DNS to Control Infected Windows PCs (July 23, 2026) — https://hackread.com/new-trickbot-variant-dns-control-infected-windows-pcs/

[13] CISA/FBI/NSA/DOE Joint Advisory AA26-097A: Iranian-Affiliated Cyber Actors Targeting Operational Technology (updated July 22, 2026) — https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a

[14] Coca-Cola Suspends US fairlife Production Due to Ransomware Attack (July 17, 2026) — https://www.securityweek.com/coca-cola-suspends-us-fairlife-production-due-to-ransomware-attack/

[15] Ransomware Group Threatening to Leak Data Stolen From Coca-Cola's fairlife (July 22, 2026) — https://www.securityweek.com/ransomware-group-threatening-to-leak-data-stolen-from-coca-colas-fairlife/

[16] Data Breach Confirmed After Australian Energy Giant Origin Is Hacked (July 23, 2026) — https://www.securityweek.com/data-breach-confirmed-after-australian-energy-giant-origin-is-hacked/

[17] Ecopetrol S.A. Form 6-K: Cybersecurity Incident Disclosure (July 17, 2026) — https://www.sec.gov/Archives/edgar/data/0001444406/000129281426003810/ex99-1.htm

[18] Data Breach Reportedly Targets India's Kudankulam Nuclear Power Plant (Reuters via Al Jazeera, July 16, 2026) — https://www.aljazeera.com/news/2026/7/16/data-breach-reportedly-targets-indias-kudankulam-nuclear-power-plant

[19] H.R. 9917, the AI Kill Switch Act — sponsor-office bill text, Rep. Lieu (introduced July 23, 2026) — https://lieu.house.gov/sites/evo-subsites/lieu.house.gov/files/evo-media-document/ai-kill-switch-act.pdf

[20] Bipartisan Bill Would Give US Government a "Kill Switch" for AI Models After Hugging Face Hack (July 23, 2026) — https://www.cnbc.com/2026/07/23/open-ai-hugging-face-hack-kill-switch-bill-congress.html

[21] Hugging Face Used Chinese Open-Weight Model for Incident Response After US Models Refused (July 24, 2026) — https://www.cnbc.com/2026/07/24/chinese-ai-model-openai-cyber-attack.html

[22] When the Sandbox Won't Hold: Lessons From Hugging Face (July 24, 2026) — https://www.healthcareinfosecurity.com/when-sandbox-wont-hold-lessons-from-hugging-face-a-32327

[23] After Hugging Face Breach, FedRAMP Chief Tells Slow-to-Patch Vendors to Stay Out of Government (July 23, 2026) — https://www.nextgov.com/cybersecurity/2026/07/after-hugging-face-breach-fedramp-chief-tells-slow-patch-vendors-stay-out-government/414972/

[24] Manifold Security: Claude for Chrome Extension Bypass (July 14, 2026; updated July 26, 2026) — https://www.manifold.security/blog/claude-for-chrome-extension-bypass

[25] Tego AI Discloses Second Claude Flaw in a Week (July 24, 2026) — https://hackread.com/tego-ai-discloses-second-claude-flaw-in-a-week-hidden-link-silently-sends-files-to-attackers/

[26] New Dolphin X Malware Uses AI Profiler to Rank High-Value Victims (July 24, 2026) — https://hackread.com/dolphin-x-malware-ai-profiler-rank-victims/

[27] OpenAI: Health in ChatGPT (July 2026) — https://openai.com/index/health-in-chatgpt/

[28] ChatGPT Wants Access to Your Health Records (July 24, 2026) — https://www.theregister.com/ai-and-ml/2026/07/24/chatgpt-wants-access-to-your-health-records-so-it-can-be-a-better-not-doctor/5278430

[29] Patient Sues Abbott Labs, Exact Sciences in Data Theft (July 24, 2026) — https://www.healthcareinfosecurity.com/patient-sues-abbott-labs-exact-sciences-in-data-theft-a-32326

[30] Kerner et al. v. Nissan North America Inc., No. 3:26-cv-00903 (M.D. Tenn.), complaint (filed July 1, 2026) — https://storage.courtlistener.com/recap/gov.uscourts.tnmd.110031/gov.uscourts.tnmd.110031.1.0.pdf

[31] NY Attorney General: $18 Million Multistate Settlement With 23andMe (July 14, 2026) — https://ag.ny.gov/press-release/2026/attorney-general-james-secures-18-million-23andme-failing-protect-customers

[32] State AGs Reach Novel Multistate Settlement With Genetic Testing Company 23andMe (Troutman Pepper Regulatory Oversight, July 22, 2026) — https://www.regulatoryoversight.com/2026/07/state-ags-reach-novel-multistate-settlement-with-genetic-testing-company-23andme/

[33] HHS Office for Civil Rights Breach Portal: OpenLoop Health, Inc. (reported March 17, 2026) — https://ocrportal.hhs.gov/ocr/breach/breach_report_hip.jsf

[34] What the OpenLoop Breach Reveals About Third-Party Healthcare Data Risk (vendor commentary, Sentra, July 26, 2026) — https://www.cybersecurity-insiders.com/what-the-openloop-breach-reveals-about-third-party-healthcare-data-risk/

[35] Ernst & Young Discloses Data Breach After Support System Hack (July 17, 2026) — https://www.bleepingcomputer.com/news/security/ernst-and-young-discloses-data-breach-after-support-system-hack/

[36] AI Music Generator Suno Breach Affects 55M Users, Per Have I Been Pwned (July 21, 2026) — https://techcrunch.com/2026/07/21/ai-music-generator-suno-breach-affects-55m-users-per-have-i-been-pwned/

[37] ShinyHunters Data Leaks Fuel $2,000 Sextortion Email Scam (July 25, 2026) — https://www.bleepingcomputer.com/news/security/shinyhunters-data-leaks-fuel-2-000-sextortion-email-scam/

[38] Major Video Doorbell Companies Are Being Sued for Privacy Violations (July 25, 2026) — https://www.cnet.com/home/security/major-video-doorbell-companies-are-being-sued-for-privacy-violations-heres-why/

[39] United States v. Belmonte Cardozo, No. 25-4239 (4th Cir. July 13, 2026), published opinion — https://www.ca4.uscourts.gov/opinions/254239.P.pdf

[40] The Fourth Circuit Says Border Agents Can Search Your Phone By Hand, No Suspicion Required (EFF, July 22, 2026) — https://www.eff.org/deeplinks/2026/07/fourth-circuit-says-border-agents-can-search-your-phone-hand-no-suspicion-required

[41] The ACLU Is Arming Lawyers to Expose State Surveillance Secrets (WIRED, July 20, 2026) — https://www.wired.com/story/the-aclu-is-arming-lawyers-to-expose-state-surveillance-secrets/

[42] US Government Targets Cop City Protester Over Phone Operating System (The Guardian, July 23, 2026) — https://www.theguardian.com/us-news/2026/jul/23/cop-city-protester-phone

[43] Flock Safety Unveils Alpha Drone as First Responder System (October 16, 2025) — https://www.flocksafety.com/blog/flock-safety-unveils-alpha-drone-as-first-responder-system

[44] SaiFlow: The Hidden CCS2 Attack Surface on EV Chargers (June 3, 2026) — https://www.saiflow.com/blog/the-hidden-ccs2-attack-surface-on-ev-chargers

[45] Mozilla Foundation: “Privacy Nightmare on Wheels” — Every Car Brand Reviewed Flunks Privacy Test (September 6, 2023) — https://www.mozillafoundation.org/en/blog/privacy-nightmare-on-wheels-every-car-brand-reviewed-by-mozilla-including-ford-volkswagen-and-toyota-flunks-privacy-test/

[46] New Jersey A5328 (data broker registration and sensitive-data sale ban; signed June 30, 2026) — https://pub.njleg.state.nj.us/Bills/2026/A5500/5328_R1.HTM

[47] US House Votes to Extend Cyber Sharing Law for 10 Years (July 24, 2026) — https://www.healthcareinfosecurity.com/us-house-votes-to-extend-cyber-sharing-law-for-10-years-a-32329

[48] SBA Office of Advocacy: Roundtable on DoW’s RFI for the CMMC Reform Task Force, July 30, 2026 (July 23, 2026) — https://advocacy.sba.gov/2026/07/23/roundtable-on-dows-rfi-for-the-cmmcs-reform-task-force-july-30-2026/

[49] SBA Office of Advocacy: DoW Requests Information for CMMC Reform Task Force (July 20, 2026) — https://advocacy.sba.gov/2026/07/20/dow-requests-information-for-cmmc-reform-task-force/

[50] Department of War Suspends CMMC Phase II Requirements, But Cybersecurity Obligations Remain (Morgan Lewis, July 2026) — https://www.morganlewis.com/pubs/2026/07/department-of-war-suspends-cmmc-phase-ii-requirements-but-cybersecurity-obligations-remain

[51] CERT-UA Advisory: UAC-0099 Fake Notepad++ Plugin Campaign (July 2026) — https://cert.gov.ua/article/6318634

[52] GAO-26-107693: Aviation Cybersecurity — FAA and TSA Are Collaborating on Cybersecurity but Need to Address Key Shortfalls (July 16, 2026) — https://www.gao.gov/products/gao-26-107693

[53] Lawmakers Get a Taste of AI-Enabled Cyberattacks in China-Taiwan War Game (July 22, 2026) — https://www.nextgov.com/cybersecurity/2026/07/lawmakers-get-taste-ai-enabled-cyberattacks-china-taiwan-war-game/414938/

[54] Manufacturers Face New Cyber Risks From Connected Factories (SonicWall 2026 Manufacturing Protect Brief, July 22, 2026) — https://www.prnewswire.com/news-releases/sonicwall-research-finds-manufacturing-cybersecurity-at-a-breaking-point-as-factory-floors-and-corporate-networks-collide-302831538.html

[55] North Korea Arrests Hackers Accused of Laundering Stolen Funds From Country’s Bank via Crypto (July 25, 2026) — https://www.coindesk.com/business/2026/07/25/north-korea-arrests-hackers-accused-of-laundering-stolen-funds-from-country-s-bank-via-crypto

[56] Scaleway Secures European Trusted Cloud Services Contract With Airbus (July 16, 2026) — https://www.scaleway.com/en/news/scaleway-secures-european-trusted-cloud-services-contract-with-airbus/

[57] Airbus Migrating 70 Critical Apps From AWS to France’s Scaleway Amid Digital Sovereignty Push (The Register, July 16, 2026) — https://www.theregister.com/paas-and-iaas/2026/07/16/airbus-migrating-70-critical-apps-from-aws-to-frances-scaleway-amid-digital-sovereignty-push/5272373

[58] OpenAI Took Ten Days to Tell Hugging Face Its Models Were Behind the July 11 Weekend Hack (Tom's Hardware, July 2026) — https://www.tomshardware.com/tech-industry/artificial-intelligence/openai-took-ten-days-to-tell-hugging-face-its-models-were-behind-the-july-11-weekend-hack

[59] US and Saudi Arabia Announce Nuclear Cooperation Deal (Al Jazeera, July 22, 2026) — https://www.aljazeera.com/news/2026/7/22/us-and-saudi-arabia-announce-nuclear-cooperation-deal

Additional Resources

- CISA Known Exploited Vulnerabilities catalog — https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- HHS OCR breach portal (verify vendor breach filings) — https://ocrportal.hhs.gov/ocr/breach/breach_report_hip.jsf
- Have I Been Pwned (Suno and other breach lookups) — https://haveibeenpwned.com
- WaterISAC (water-sector threat intelligence) — https://www.waterisac.org

---

Prepared by The Stillwater Group in partnership with Datec. The Stillwater Group provides cybersecurity advisory services to organizations across critical infrastructure, public, and private sectors. Datec provides enterprise infrastructure solutions, system integration, and technical professional services across data center, networking, and security platforms. Contact us with questions about this briefing or to discuss your organization's specific risks and infrastructure needs.

Stillwater

Kevin Rolnick, Sales & Partnerships Executive
kevin@stillwater.io
www.stillwater.io
+1-425-818-1745

DATEC INCORPORATED

Cliff McElroy, President
206-419-0098
cliffm@datecinc.net
www.datecinc.net