SANCTIR WORKING PAPER · WP-2026 SERIES

Data Center Cybersecurity Against Nation-State Operations

Architecture, Technology, Assurance and Cost for 100–300 MW Campuses

What a state actor holding valid administrator credentials can reach on a reference campus, how long it stays, which rules reach the facility, and the configuration and cost of a program built to limit the consequence

PUBLISHED
23 OCTOBER 2026

STATUS
WORKING PAPER — SSRN

EVIDENCE
SOURCES READ 11–23 OCTOBER 2026

VERSION
1.0

AUTHOR
COLLIN B. GEORGE, CISSP

LICENSE
CC BY-NC-ND 4.0

UNCLASSIFIED // OPEN SOURCE

Paper record

ABSTRACT

A 100–300 MW data center campus should be designed on the assumption that a state intelligence service will at some point hold valid administrator credentials inside its management networks. This paper assembles the public record behind that assumption and works out what follows for architecture, technology, assurance and cost. The documented entry methods since 2021 are few and they repeat: internet-facing routers, firewalls and VPN gateways; identity keys and tokens with broad scope and long life; appliances that cannot run endpoint detection; and suppliers who hold access to their customers. Dwell times are measured in years rather than days, and exploitation on average precedes the patch, so patching cannot be the main control for an exposed system. The facility systems are weak and now matter to the grid, while no cyber rule reaches the facility as a data center: the July 2026 FERC order, the NERC alerts and the three computational-load standards that passed final ballot in October 2026 contain no cyber security requirement beyond a secure-transfer method. Confidential computing does not remove the operator from the trust boundary; five published attacks between December 2024 and September 2026 defeated AMD and Intel protections with brief physical access and inexpensive hardware. Because a defense cannot depend on knowing the technique, the paper derives eight design principles that limit consequence instead, sets out a recommended configuration and implementation sequence, and models the cyber and control-system program of a stand-alone 200 MW campus at 28–29 security staff and $9–14 million a year.

KEYWORDS

data center security; critical infrastructure; nation-state intrusion; operational technology; confidential computing; supply chain assurance; grid reliability; NERC CIP

JEL CLASSIFICATION

L86 (Information and Internet Services; Computer Software); L94 (Electric Utilities); H56 (National Security and War); K23 (Regulated Industries and Administrative Law); O33 (Technological Change: Choices and Consequences)

SCOPE

Companion to Data Center Design, Resilience, Reliability and Sustainability: Power, Cooling, Redundancy and Cost for 100–300 MW Campuses in Virginia (the “design paper”). Sources were opened on 11, 12, 22 and 23 October 2026 with AI research assistance and are linked in the text. It has had several rounds of external review, a citation audit of every link, targeted primary-source checks and a refresh of its time-sensitive statements on 22 and 23 October 2026 (Appendices A–C), and the author has read each source. Section 15 lists what is verified, what rests on secondary sources, and what could not be opened. License: CC BY-NC-ND 4.0.

IF YOU READ NOTHING ELSE

What to assume	A 100–300 MW data center campus should be designed on the assumption that a state intelligence service will at some point hold valid administrator credentials inside its management networks. The documented entry methods since 2021 are few and they repeat: internet-facing routers, firewalls and VPN gateways; identity keys and tokens with broad scope and long life; appliances that cannot run endpoint detection; and suppliers who hold access to their customers.
Why it matters now	Dwell times are measured in years rather than days, and exploitation on average precedes the patch, so patching cannot be the main control for an exposed system. The facility systems are weak and now matter to the grid, while no cyber rule reaches the facility as a data center: the July 2026 FERC order, the NERC alerts and the three computational-load standards that passed final ballot in October 2026 contain no cyber security requirement beyond a secure-transfer method.
What to build	Confidential computing does not remove the operator from the trust boundary; five published attacks between December 2024 and September 2026 defeated AMD and Intel protections with brief physical access and inexpensive hardware. Because a defense cannot depend on knowing the technique, the paper derives eight design principles that limit consequence instead, sets out a recommended configuration and implementation sequence, and models the cyber and control-system program of a stand-alone 200 MW campus at 28–29 security staff and $9–14 million a year.

1 Executive summary

A 100–300 MW data center campus should be designed on the assumption that a state intelligence service will at some point hold valid administrator credentials inside its management networks. The public record supports that assumption. The design question is what such an actor can then do, and how long it can stay.

How state actors get in. The documented entry methods since 2021 are few and they repeat: internet-facing routers, firewalls and VPN gateways; identity keys and tokens with broad scope and long life; hypervisor managers and other appliances that cannot run endpoint detection; and suppliers who hold access to their customers. Google attributed just over half of state-espionage zero-day exploitation in 2025 to edge devices and security appliances. Agencies of thirteen countries reported that they had not observed Salt Typhoon using any zero-day. Known flaws and stolen credentials were enough.

How long they stay. U.S. agencies observed Volt Typhoon holding access for at least five years. Google and Mandiant measured an average of 393 days for intrusions using the BRICKSTORM backdoor. Mandiant measured a mean time to exploit of about minus seven days in its 2025 sample, meaning that on average exploitation preceded the patch. Verizon reports that only 26% of known exploited flaws were fully remediated, with a 43-day median. Patching cannot be the main control for an exposed system, and 90 days of logs cannot reconstruct an intrusion of this length.

The facility systems are weak, and they now matter to the grid. Claroty's 2026 telemetry found 18% of data center infrastructure devices one network connection away from a system making risky outbound connections to the internet, and 88% of building management systems using insecure protocols. In Poland on December 29, 2025, attackers used default accounts to disable remote terminal units and two protection relays across at least 30 sites. On July 22, 2026, about 3,900 MW of Dominion-zone data center load transferred to backup power after an ordinary fault, about 2,900 MW at once and about 1,000 MW a minute later. That event was not a cyber event. It shows the size of load a coordinated command to transfer or island could move. Whether a commanded transfer would produce the same voltage and frequency excursion has not been modeled in public. About sixteen campuses of the reference size equal it.

No cyber rule covers the facility as a data center. FERC's July 16, 2026 order on computational loads and NERC's two alerts contain no cyber security requirement, and NERC's three draft standards, read in their first formal posting and in the final-ballot text that passed on October 14, 2026, contain none beyond a requirement that each grid operator's data specification include a mutually agreeable method for secure transfer. Data centers are not a separate critical infrastructure sector. The federal incident-reporting rule is not yet published. Obligations reach an operator only indirectly, through electric reliability registration, securities law, contracts and foreign law. For the facility itself the baseline is voluntary or set by tenant contract.

Confidential computing does not remove the operator from the trust boundary. Five published attacks between December 2024 and September 2026 defeated AMD SEV-SNP, Intel TDX or Intel SGX protections using brief physical access and $10 to $1,000 of hardware, in two cases together with control of the host software. AMD fixed the first, BadRAM, in firmware. For the other four, AMD and Intel treat physical attacks as outside their threat models; AMD plans no mitigation and Intel has issued none. The attacks were shown on particular processor generations and memory types, listed in Section 7. A tenant's protection against the facility operator, an insider or an interdictor rests on physical controls the tenant can audit.

Attacks not yet known. Automated systems now find software flaws in volume. A defense cannot depend on knowing the technique. It can limit the consequence. Eight design principles follow from that (Section 5): limit what any digital command can do; remove reachability; make trust short-lived and verifiable; require two people for irreversible or site-wide actions; keep evidence where an intruder cannot erase it; hold the means of recovery under a separate authority; verify control-system reports with independent measurement; and keep the ability to run power and cooling by hand.

Recommendation. Build the campus to the configuration in Section 14. Its main elements: no management interface reachable from the internet; a physically separate management network; hardware-bound administrator authentication with two-person approval for site-wide commands; a higher security target for the protection, microgrid and battery control zones than the design paper set; hardwired limits on transfer, islanding and battery output; one-way data transfer out of control zones; server and controller firmware that can be measured and recovered; 24 months of protected logs;

recovery images and spares held outside the production authority; and physical controls on hands-on server work that a tenant can audit.

Cost. The author's model for the cyber and control-system program of a stand-alone 200 MW campus is 28–29 security staff and $9–14 million a year, about $4.50–7.00 per MWh of facility energy, excluding physical guarding. The design paper's resilience premium was about $23 per MWh. These are engineering estimates with stated inputs (Section 13). No public unit prices were found for most of the equipment.

Status of this version. Sources were opened on October 11, 12, 22 and 23, 2026 with AI research assistance and are linked in the text. It has had several rounds of external review, a citation audit of every link, targeted primary-source checks and a refresh of its time-sensitive statements on October 22 and 23 (Appendices A–C). The author has read each source. Section 15 lists what is verified, what rests on secondary sources, and what could not be opened.

2 Scope, method and relationship to the design paper

This paper covers the systems a campus operator controls. It treats the tenant's applications as out of scope, except where a facility decision settles the tenant's exposure.

In scope.

- Facility controls: protective relays, power monitoring, paralleling switchgear, engine controls, the battery plant, the microgrid controller, the building management system (BMS), data center infrastructure management (DCIM), coolant distribution units (CDUs) and heat rejection.
- The operator's management planes: the out-of-band network, server baseboard management controllers (BMCs), the hypervisor and orchestration control plane, identity systems and physical access control.
- The network edge, interconnection and time sources.
- The supply of hardware, firmware, software and services.
- For operator-run compute, the server platform up to the tenant boundary, including the protection of AI model weights.

Reference design. The design paper's reference campus is used unchanged: 200 MW of IT load and about 240 MW at peak; two 230 kV lines; sixteen 20 MW dual-fuel engines arranged N+2; a 120 MW / 240 MWh grid-forming battery; engines and battery connected at 34.5 kV under a microgrid controller that can island the campus; direct-to-chip liquid cooling with CDUs and dry coolers. Section 10 of the design paper set the control-system baseline: Purdue-model segmentation with ISA/IEC 62443 zones, security level 2 for mechanical controls and level 3 for electrical controls, a control-system DMZ, one-way gateways, brokered vendor access, passive monitoring and hardwired protective trips. This paper keeps that baseline and extends it to the IT, identity, platform and supply sides. It revises one item, the security target for three control zones (Section 6).

Adversary. The planning adversary is a state service or a contractor working for one. RAND's 2024 study of AI model-weight security gives a usable scale. Its fourth class is a standard operation by a leading cyber-capable institution: about 100 people, a year, and up to $10 million. Its fifth class is a top-priority operation: about 1,000 people, years, and up to $1 billion (RAND RR-A2849-1). Three objectives are considered: espionage against tenant data and model weights; pre-positioning for later disruption; and disruption or destruction.

Jurisdiction. The threat does not depend on location. The legal analysis is United States federal law, with Virginia and three foreign comparators.

Method. Factual statements are linked to their sources where they are first made; later sections refer back to them. Government sources and vendor research are distinguished, and each attribution names who made it. Where sources conflict, both figures are given. Where the record is silent, the paper says so; the absences that matter are stated at the end of Section 3. Figures labeled as the author's estimate are engineering estimates.

Research assistance and its limits. Sources were located and opened on October 11, 12, 22 and 23, 2026 with AI research assistance. Quotations were checked against the source pages by the author. Two limits follow. Coverage of 2026 events is incomplete, because the search allowance was exhausted before every question was closed. Several primary documents could not be opened and are cited through secondary sources, each marked in Section 15. The design paper went through five external review rounds and a citation audit. This paper has had four external rounds and two citation audits, recorded in Appendices A–C.

3 The threat record, 2015–2026

State actors have entered infrastructure networks through a small number of repeated methods, and they have stayed for years. The Office of the Director of National Intelligence calls China "the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks" and says China and Russia are continuing their pre-positioning efforts (ODNI, March 2026).

Entry methods on the IT side. The table lists the methods documented by governments or by established incident-response firms. Attribution is by the named source.

Entry method	Documented cases	Source
Internet-facing routers, firewalls and VPN gateways	Volt Typhoon exploited known or zero-day flaws in public-facing network appliances. Salt Typhoon used known flaws only; no zero-day use was observed. A Cisco firewall actor modified device read-only memory to persist through reboot and upgrade. A Cisco SD-WAN campaign exploiting a controller flaw, CVE-2026-20127, ran from at least 2023.	CISA AA24-038A; joint advisory, Aug. 2025; CISA ED 25-03; Cisco Talos, Feb. 2026

Entry method	Documented cases	Source
Valid credentials on network devices and administration hosts	Salt Typhoon's access to Cisco devices came mainly from stolen legitimate credentials. UNC3886 reached Juniper routers from a terminal server used to manage network devices, with legitimate credentials.	Cisco Talos, Feb. 2025; Mandiant, March 2025
Identity keys and tokens	Storm-0558 forged tokens with a signing key Microsoft created in 2016 and reached the mailboxes of 22 organizations. Midnight Blizzard entered Microsoft through a test tenant account without multifactor authentication and then abused an OAuth application. Silk Typhoon used API keys stolen from privileged-access and IT providers to reach their customers.	CSRB report; Microsoft, Jan. 2024; Microsoft, March 2025
Hypervisor managers and appliances that cannot run endpoint detection	UNC3886 exploited a VMware vCenter flaw from late 2021, about a year and a half before it was patched. BRICKSTORM operators deployed a tool able to capture vCenter logins and cloned the virtual machines of domain controllers and secret vaults. A Dell replication appliance flaw, CVE-2026-22769, was exploited from mid-2024.	Mandiant, Jan. 2024; Google GTIG, Sept. 2025; Google GTIG, Feb. 2026
Server management controllers (BMCs)	CVE-2024-54085, an authentication bypass in AMI MegaRAC firmware, was added to CISA's exploited list on June 25, 2025. The exploiting party is not identified.	NVD; Eclypsium
Suppliers	SolarWinds updates were altered by the Russian foreign intelligence service. A state actor gained long-term access to F5 BIG-IP source code and undisclosed vulnerability information. An internet service provider was compromised to redirect insecure software-update requests through altered DNS answers.	GAO-22-104746; F5, Oct. 2025; Volexity, Aug. 2024

Google's count for 2025 is 90 zero-days exploited in the wild, 43 of them in enterprise software and appliances. State espionage groups focused just over half of their attributed zero-day exploitation on edge devices and security appliances (Google GTIG, March 2026). After entry, the actors move to the identity system. Volt Typhoon extracted the Active Directory database and relied on valid credentials afterward. In one BRICKSTORM case documented by CISA, NSA and the Canadian Centre for Cyber Security, the actors exported cryptographic keys from the federation server and also reached vCenter (AR25-338A).

Time. These intrusions last longer than most organizations keep logs.

Case	Duration of access	Source
Volt Typhoon, some victims	At least 5 years	CISA AA24-038A
Cisco SD-WAN campaign	At least 3 years	Cisco Talos
Salt Typhoon, one victim	Over 3 years	Cisco Talos

Case	Duration of access	Source
BRICKSTORM victim documented by CISA	April 2024 to at least September 3, 2025, about 17 months	AR25-338A
BRICKSTORM intrusions, average	393 days	Google GTIG and Mandiant; M-Trends 2026 executive edition
Espionage cases, median, 2025	122 days	Mandiant M-Trends 2026
All intrusions, median, 2025	14 days	Mandiant M-Trends 2026

The rows measure different things: single victims, a campaign average and medians across all investigations. They are not one distribution. Mandiant reports the same 122-day median for espionage cases and for North Korean IT-worker cases. Two other measurements matter. Mandiant estimates the mean time to exploit at about minus seven days and reads this as exploitation routinely occurring before a patch is released. A mean does not show what share of flaws are exploited before a patch exists. Verizon found that only 26% of flaws on CISA's exploited list were fully remediated, with a median of 43 days (Verizon DBIR 2026). Mandiant states the consequence: with dwell times near 400 days, 90-day log retention leaves an organization unable to see how the intrusion began. Several of the actors also kept access after the victim patched. The Cisco firewall actor altered read-only memory, and a Dutch government review found FortiGate access that persisted after updates (NCSC-NL).

Control systems. State attacks on control systems follow a consistent sequence: entry through the business network, a VPN or an exposed device; use of the control system's own functions; then damage to field devices to slow recovery.

- Ukraine, December 2015. Attackers opened breakers from the operators' own control screens, cut power to about 225,000 customers, loaded damaging firmware onto serial-to-Ethernet gateways and reconfigured an uninterruptible power supply (SANS and E-ISAC). The U.S. Department of Justice charged six Russian military intelligence officers (DOJ, 2020).
- A refinery safety system. U.S. agencies attribute the TRITON malware, built to manipulate Schneider Triconex safety controllers, to a Russian state research institute. The refinery shut down for several days (CISA, FBI and DOE, AA22-083A).
- Ukraine, October 2022. Mandiant reports that Sandworm reached a substation control system through a hypervisor and likely tripped breakers using a program that was part of the control product itself. The control-system part of the attack may have taken as little as two months to develop (Mandiant).
- Ukraine, January 2024. Modbus commands to heating controllers cut heat to more than 600 apartment buildings in sub-zero weather. Entry was possibly through an exposed router. Dragos names no actor (Dragos).

- Poland, December 29, 2025. At least 30 wind and solar sites and two combined heat and power plants were attacked. Entry was through FortiGate VPN accounts without multifactor authentication. Default accounts then gave access to field devices. Hitachi remote terminal units were left in a reboot loop by corrupted firmware, and two Hitachi protection relays could not be restarted. Generation continued. A second plant was entered through a controller on a private cellular network run by the distribution operator (CERT Polska report; follow-up). Attribution is disputed. CERT Polska points to infrastructure used by the cluster known as Static Tundra or Berserk Bear. Dragos assesses with moderate confidence that it was ELECTRUM (Dragos).
- United States, from March 2026. Six U.S. agencies report Iranian-affiliated actors manipulating internet-facing programmable logic controllers in government facilities, water systems and energy organizations, in a few cases with operational disruption and financial loss. They say the escalation is likely a response to hostilities between Iran and the United States and Israel (AA26-097A). A July 22 update, co-sealed by seven agencies with the addition of the Treasury, reports that at one U.S. victim the actors downloaded a malicious project file and that modified logic disabled critical shutdown and alarm logic (AA26-097A update; also Industrial Cyber).

Volt Typhoon belongs in the same list as a capability. U.S. agencies observed the actors testing access to control systems with default vendor credentials. They name manipulation of heating, ventilation and air conditioning in server rooms as a possible effect (CISA AA24-038A).

Data center facility systems. Published research documents serious flaws in representative products of each main class of facility system a campus uses, except coolant distribution units.

System class	Finding	Source
DCIM software and rack power distribution units	Nine flaws in CyberPower and Dataprobe products, including authentication bypass. The researchers judged that an intruder could cause disruption lasting days.	Trellix, 2023
DCIM software	Schneider EcoStruxure IT Data Center Expert: command injection rated 10.0.	CISA ICSA-25-203-06
UPS network cards	Vertiv Liebert cards: authentication bypass and buffer overflow, both rated 9.8.	CISA ICSA-25-140-10; Claroty, June 2026
Chiller and HVAC controllers	Trane Tracer SC+: a chain allowing remote code execution without authentication.	Claroty, June 2026
Building management frameworks	Tridium Niagara: ten CVEs, exploitable where encryption is misconfigured.	Nozomi Networks, 2025

Two 2026 measurements describe how reachable these systems are. Claroty analyzed more than 750,000 devices in large data centers. It states that 0.4% of infrastructure devices are directly exposed to the internet, though its own counts give about 0.6%, and that 18% are one connection away from a

system making risky outbound connections to the internet (Claroty report; Claroty summary). It found that 88% of building management systems and 86% of UPS units use insecure protocols (Claroty, July 2026). Trend Micro's research unit found 6,300 control-system devices reachable from the internet within one kilometer of more than 1,000 U.S. data center locations, 58% of them using BACnet. The authors state that they cannot confirm any of these devices belongs to a data center (TrendAI Research, Aug. 2026).

Load as a grid effect. Three Dominion-zone events show what a simultaneous transfer of data center load does. None was a cyber event.

Date	Load transferred	Grid effect	Source
July 10, 2024	About 1,500 MW	Frequency rose to 60.047 Hz; voltage to 1.07 per unit	NERC incident review
February 17, 2025	About 1,800 MW in PJM's September 2026 account; about 1,500 MW in its first report	Frequency to about 60.042 Hz; voltage to about 1.05 per unit	PJM; PJM Planning Committee
July 22, 2026	About 3,900 MW (about 3,800 MW in PJM's first report): about 2,900 MW, then about 1,000 MW a minute later	Frequency reached 60.092 Hz; voltage to about 1.14 per unit; high voltage caused the second round of transfers	PJM Operating Committee

In all three events, protection and transfer settings inside the data centers moved the load to backup after faults on 230 kV lines: a failed lightning arrester in 2024, a sustained single-line-to-ground fault cleared in 5.9 cycles in 2025, and a mechanical failure in 2026 (PJM Planning Committee, Sept. 15, 2026). PJM reported no relay misoperation in 2026 and attributed the transfers likely to voltage ride-through performance. No public Dominion root-cause analysis of the 2026 event, which Dominion said would be completed in September 2026, was located on October 22. A party able to command the same transfer or an islanding operation at many sites at once could remove load of the same size without a fault. Whether the voltage and frequency excursion would match depends on sequence, location and system conditions, and no public study has modeled it. No source reports that this has occurred. PJM has proposed ride-through requirements for large loads in response to a FERC order of June 18, 2026 (Docket EL26-67-000): load must return above 90% of its pre-disturbance level within 2 seconds after voltage recovers and stay within 10% of it through frequency deviations, and cooling load may trip below 0.35 per unit. PJM targets a filing in November 2026 (PJM Planning Committee, Sept. 8, 2026). NERC opened a further standards project on computational load disturbance performance, covering voltage and frequency ride-through and post-fault active power recovery; its authorization request was accepted on October 21, 2026 and posted for comment through November 20 (NERC Project 2026-03). NERC's January 2026 CIP Roadmap lists large loads among growing exposures that are outside enforceable cyber standards, and it recommends continued monitoring (NERC).

Automation and the rate of discovery. Three kinds of evidence exist, and they differ in reliability.

- One state operation. Anthropic reported that a group it assesses with high confidence to be Chinese state-sponsored used an AI coding agent against about 30 targets, with the agent doing an estimated 80–90% of the tactical work (Anthropic, Nov. 2025). The report comes from the vendor whose model was misused.
- Measured discovery. In DARPA's AI Cyber Challenge final, automated systems found 54 of 63 planted flaws and 18 real ones, at an average cost of about $152 per task (DARPA, Aug. 2025). Anthropic states that partners using its restricted model found at least 129,000 verified software flaws between April and July 2026 (Anthropic, Oct. 2026). That figure is self-reported. The UK AI Security Institute found that the same model completed a 32-step simulated network attack in 3 of 10 attempts, in a test range with no active defenders, and could not complete a control-system range (UK AISI, April 2026).
- Observed adversary use. Google reported in February 2026 that it had not yet seen state actors achieve breakthrough capabilities with AI (Google GTIG). Mandiant does not regard 2025 as a year in which breaches were the direct result of AI. NSA said on October 8, 2026 that adversaries are using what it calls super intelligence capabilities to automate reconnaissance and speed exploit development (NSA).

The planning conclusion is limited. More flaws will be found faster, by defenders and attackers alike, in the appliance and management software a campus runs. No opened source measures state exploitation of machine-discovered flaws at scale.

What the record does not show. Four absences should be stated plainly.

1. No opened source documents a named data center whose power or cooling was taken out of service by a cyber intrusion. The nearest items are an unverified April 2026 claim by a Russian hacktivist group, relayed by Claroty, and vendor statements about access to DCIM and BMS environments.
2. No official source confirms that Salt Typhoon compromised a data center or colocation operator. One press report, citing three unnamed people familiar with the matter, says CISA listed Digital Realty as potentially compromised (Nextgov, June 2025). The joint advisory does describe abuse of peering and private interconnection links.
3. No opened source attributes a server BMC implant to a named state.
4. The U.S. Department of Energy's laboratory review of about 30 inverters found no definitive evidence of malicious hidden radios, according to trade press (pv magazine USA, Jan. 2026). The May 2025 Reuters report of undocumented communication devices in some Chinese inverters and batteries, read here in a syndicated copy, rested on two unnamed sources.

No research on vulnerabilities in coolant distribution unit controllers was found. That is an absence of research, not evidence of security.

4 What an intruder can reach on the reference campus

The campus has three kinds of consequence, and the same intrusion can produce more than one. A site consequence is loss of power or cooling to the halls. A tenant consequence is theft or alteration of tenant data, including model weights. A grid consequence is a sudden change in 240 MW of load, or in the output of 320 MW of engines and a 120 MW battery, nameplate, with export limited by the interconnection agreement.

The table maps each system to what an intruder with administrative access could do and to the nearest precedent in Section 3. The third column is the author's analysis.

System	Nearest precedent	What administrative access allows	Consequence
Internet and WAN routers, firewalls, VPN gateways, load balancers	Volt Typhoon, Salt Typhoon, the Cisco firewall and SD-WAN campaigns	Long-term presence, traffic capture, a base for entering management networks	Tenant; site by onward movement
Directory, federation, certificate authority, privileged-access system	Storm-0558, Midnight Blizzard, the CISA BRICKSTORM case	Forged tokens and certificates; administrator rights on every dependent system	All three
Out-of-band network and server BMCs	CVE-2024-54085; OpenBMC and HPE iLO 7 flaws of September and October 2026	Power control and firmware replacement on every server; Eclypsium describes reboot loops the victim cannot stop	Site; tenant
Hypervisor manager, orchestration control plane, job scheduler	UNC3886, BRICKSTORM	Copying of virtual machines and secrets; control of when the IT load runs	Tenant; grid
DCIM, BMS and power monitoring	Trellix, Claroty, CISA advisories	False readings to operators; commands to power distribution units, UPS units and cooling plant	Site
CDUs, dry coolers, trim chillers	Trane and Niagara findings; no CDU research found	Loss of coolant flow or heat rejection to racks above 100 kW	Site
UPS units, static transfer switches, rack power distribution	Ukraine 2015; Claroty findings	Transfer or shutdown of IT load	Site; grid if widespread
Microgrid controller, paralleling switchgear, engine controls, battery plant controller	Ukraine 2022; Poland 2025	Islanding, reconnection, dispatch, changes to ramp rates and operating limits	Site; grid

System	Nearest precedent	What administrative access allows	Consequence
Protective relays and their settings	Poland 2025; the July 2026 event	Disabling of relays; setting changes that cause or prevent trips	Site; grid
Utility telemetry and the operating links that NERC's draft standards would add	The Polish private cellular network case	Entry to control zones through a network someone else manages	Site; grid
Time sources	None found in this research	Loss or falsification of time for protection, event recording and IT clocks	Site
Physical access control and video	None found in this research	Entry to halls and cages; removal of evidence	Tenant
Vendor remote access and managed services	Silk Typhoon; the Polish VPN accounts	The vendor's access, used by someone else	All three
GPU software, fabric manager, network card firmware	Four flaws in the NVIDIA Container Toolkit in 21 months, three of them container-to-host; a 2026 flaw in NVIDIA's fabric management software	Movement from one tenant to the host or to another tenant	Tenant

Three points follow from the table.

An IT compromise can cause a site outage without touching the control systems. The BMC network can power off or disable every server. A campus whose power and cooling controls are well isolated can still be stopped through the management network.

An IT compromise can cause a grid effect. In an AI campus the job scheduler decides when 200 MW of load runs. Synchronized starts and stops across training clusters are load steps. A data center developer's presentation to NERC's large-loads task force lists AI training ramps and oscillations as an operating concern, and a Pacific Northwest National Laboratory slide in the same materials states that data center load can fluctuate periodically and force oscillations in the grid (NERC LLTF, Aug. 2025). That a compromised scheduler could be used this way is the author's inference. No source reports it.

The grid-scale risk is a common mode, not one campus. One reference campus is 240 MW. The July 2026 event was about 3,900 MW, or about sixteen such campuses. The condition that would let one actor command sixteen is shared equipment or shared access: the same microgrid controller or UPS product with the same flaw, the same vendor's remote-access service, or one operator's central management system. Concentration of control-system vendors and of remote access is therefore the variable to manage. No rule requires that it be measured.

Time sources. A campus with a 230 kV substation, a grid-forming battery and disturbance recorders has at least three consumers of satellite-derived time: protection and recording, power-plant control, and the IT clock service. NIST's profile for the responsible use of positioning, navigation and timing services is the applicable federal guidance (NIST IR 8323 Rev. 1). The design task is to state, for each consumer, what happens when time is lost and when it is false. This research opened no source on recent interference trends, so none is cited.

5 Design principles for attacks not yet known

A defense against unknown attacks cannot be a list of known techniques. It has to limit what a successful intruder can cause, whatever method was used to get in. Idaho National Laboratory's Cyber-Informed Engineering takes this position: it describes itself as an engineering approach that reduces the consequences of cyberattacks and treats cyber risk as an element of engineering risk management (INL). NSA's zero trust guidance states the operating assumption: defend resources as if an adversary is already present in the environment (NSA, Jan. 2026).

The eight principles below are the author's synthesis for a data center campus. Each is tied to an event in Section 3 that it would have limited.

#	Principle	What it limits	Event it answers
1	**Limit what any digital command can do.** Put the limit in wiring, mechanics or locally stored settings that the network cannot change.	The worst outcome of a fully compromised control network	TRITON; the altered controller logic reported in 2026
2	**Remove reachability.** A system that cannot be reached from a network does not depend on a patch to resist remote attack. It remains exposed to malicious updates, removable media and insiders, so patching and integrity checks continue.	Exposure during the period before a patch exists or is applied	A measured mean time to exploit of about minus seven days; a 43-day median to remediate
3	**Make trust short-lived and verifiable.** Credentials expire in hours. Keys stay in hardware. Devices prove their firmware state.	The value of anything stolen	A 2016 signing key used in 2023; keys exported from a federation server
4	**Require two people for irreversible or site-wide actions, and cap the rate of bulk actions.**	Damage from one stolen administrator identity or one insider	Wiper deployment through group policy in Poland; BMC control of all servers
5	**Keep evidence where an intruder cannot erase it, for longer than intrusions last.**	The intruder's ability to remain unseen and unreconstructed	Average dwell of 393 days against 90-day logs
6	**Hold the means of recovery under a separate authority.** Offline images, spares and backup vaults are not administered by production accounts.	Loss of the ability to rebuild	Corrupted firmware on remote terminal units; relays that would not restart

#	Principle	What it limits	Event it answers
7	**Verify what control systems report with independent measurement.**	Operator decisions made on false readings	Manipulated operator displays in the 2026 campaign
8	**Keep the ability to run power and cooling by hand, and prove it by exercise.**	Dependence on any networked system for continued operation	Ukraine 2015 and Poland 2025, where remote control of field devices was lost

Two further rules apply across all eight.

Assume the appliance is compromised, not only vulnerable. Edge and management appliances cannot run endpoint detection and have little storage for forensics. Several actors kept access through reboot, upgrade and patching. The response to a suspected compromise of such a device is replacement or a verified rebuild from the vendor's image, followed by rotation of every credential the device held.

Keep cryptography replaceable. Protocols, key sizes and trust anchors will change within the life of the facility. The post-quantum transition has dated federal requirements (Section 8). The 2026 expiry of Microsoft's 2011 Secure Boot certificates showed that a trust anchor stored in firmware needs an owner, an inventory and a renewal plan (Section 7).

These principles do not replace known-technique defenses such as patching, hardening and detection signatures. They decide what happens when those fail.

6 Facility and power-system controls

The design paper's control-system baseline stands. This section adds what the 2025–2026 record requires and revises the security target for the zones whose compromise has a grid consequence.

Security targets. ISA/IEC 62443 defines four security levels by the adversary a zone must withstand. As vendor copies of IEC 62443-3-3 quote it (the standard itself was not opened), level 2 addresses intentional violation by simple means with low resources, generic skills and low motivation; level 3, sophisticated means with moderate resources, control-system-specific skills and moderate motivation; level 4, sophisticated means with extended resources, control-system-specific skills and high motivation. The design paper set level 3 for electrical, generation and microgrid controls. A state service is a level 4 adversary. This paper therefore sets a target of level 4 for three zones: protection, microgrid and generation control, and battery plant control. This research found no microgrid controller, protection relay or battery plant controller certified to level 4; the only level 4 certification found was for a firewall operating system, as a distributor reports it. Level 4 is therefore a target, not an achieved level. The engineered limits and one-way transfer below reduce consequence. They do not by themselves establish level 4. Each zone needs an assessment against the system requirements of IEC 62443-3-3, with unmet requirements recorded as residual risk. Mechanical controls stay at level 2 on two conditions: each

cooling loop runs safely on its local controller with the BMS disconnected, and a consequence analysis shows that loss of several loops at once, through a common BMS or vendor connection, stays within the thermal margin. If it does not, the target rises to 3.

Zones.

Zone	Contents	Target	Connections allowed
Protection	Relays, hardwired trip circuits, synchronism-check relays	4	None inbound by network; settings changed only at the device; event data out through a one-way gateway
Power control	Microgrid controller, paralleling switchgear, engine controls	4	Supervisory commands from the control room only; data out one-way
Battery plant	Plant controller, power conversion systems, battery management	4	As power control; no vendor cloud link; no wireless modules
Electrical monitoring	Power monitoring system, UPS and transfer-switch supervision	3	Receives data pushed out of the zones above through their one-way gateways; does not poll into them
Mechanical	CDUs, dry coolers, trim chillers, BMS	2, with local autonomous control	BMS supervisory; no commands from DCIM
Control-system DMZ	Replicated historian, patch staging, vendor access broker, monitoring collectors	3	The only meeting point of IT and control networks; no traffic passes through it unbroken
Utility interface	Telemetry and operating links to the utility and grid operator	3	Treated as an untrusted network; ends in its own DMZ

[embedded content: Reference campus · zones and permitted connections (author’s design)]

Data leaves the control zones through one-way gateways. Commands reach them only from the control room, with two defined exceptions: the fixed list of permitted utility signals that end in the Utility interface DMZ and are enforced there, and the setting changes that engineered limit 6 allows over an authenticated connection with second-person approval. Vendors and the utility each end in a separate intermediate zone, and tenant networks connect to none of these boxes.

Engineered limits. These are the controls that still hold when every networked system is compromised.

1. Protective trips and engine safety shutdowns are hardwired and independent of every controller that can be reprogrammed over a network. The design paper already requires this.
2. Paralleling and reconnection require a synchronism-check relay in the Protection zone. The microgrid controller can request closure. It cannot force it.

3. Islanding the whole campus on command, as opposed to islanding on a protection trip, requires a hardwired permissive operated by a second person in the control room, wired independently of any operator workstation or SCADA server. The permissive applies only to commanded islanding. It never delays protective tripping, anti-islanding protection, automatic load shedding or safety functions, and its failure state is defined in the design.
4. The battery's power conversion systems enforce ramp-rate and power limits stored locally, and a change requires presence at the equipment. Converter firmware is programmable, so these limits are backed by two independent elements: a limiting function the manufacturer defines, with its own write authority separate from the converter firmware; and relays at the point of interconnection, set at the device, that trip the plant if export or rate of change leaves the design envelope. A trip is a last resort and is itself a step change, so the design studies in Section 14 must show the system can absorb it. The battery management system's own safety shutdowns remain beneath both.
5. Controller mode switches stay in the run position. Program mode is used only during a planned change with a person at the device. U.S. agencies gave this instruction for the 2026 controller campaign (AA26-097A).
6. Relay settings, UPS transfer settings and ride-through settings are changed by two people under change control, from an offline baseline, and verified electrically afterward. Change at the device is the default. Remote change is allowed only for settings the utility must be able to adjust, which are held on devices in the Utility interface DMZ or the Power control zone and never on protection relays, over an authenticated connection that a second person approves for each use. The counters and thresholds that decide when IT load moves to backup are in this class. PJM attributes the July 2026 transfers likely to ride-through performance, and its proposed ride-through rule (Section 3) will constrain them.

No default accounts at energization. In Poland, default or statically configured accounts gave the attackers access to field devices, including Hitachi RTU560 remote terminal units and Relion 650 protection relays, which were then disabled (CERT Polska). The commissioning procedure must show, device by device, that default accounts are removed, credentials are unique, and unused services such as FTP, Telnet and embedded web servers are off. This is a commissioning hold point, like a relay test.

One-way transfer and untrusted links. A joint U.S., Canadian and New Zealand guide states that hardware-enforced segmentation by unidirectional gateways or data diodes is used where cyber operations pose credible threats (CISA and partners, 2024). Data leaves the Protection, Power control and Battery plant zones only through such devices. Links that must carry commands inward, such as a utility curtailment signal, end in the Utility interface DMZ. They pass a fixed list of permitted commands and nothing else. CERT Polska's recommendation after the second plant intrusion applies directly: treat a private network run by another party as untrusted, isolate devices on it from each other, and do not expose management services to it (CERT Polska follow-up).

Wireless and vendor cloud links. Cellular and Wi-Fi modules in battery, inverter and controller equipment are disabled at commissioning by a method the manufacturer supports, or omitted by ordering a certified configuration without them, and the result is checked by inspection and a radio-frequency survey.

Physical removal from listed equipment can void its certification and is done only with the manufacturer's approval. Vendor cloud telemetry is off unless it passes through the access broker. This control does not depend on where the equipment was made. The Federal Communications Commission added foreign-produced power inverters to its Covered List on July 28, 2026, citing the possibility that a foreign firm could turn inverters off or collect data from them (FCC DA 26-786). Section 9 covers the procurement effect.

Vendor access. The design paper requires brokered, recorded, multifactor sessions with no standing connections. Three additions: each session is approved by a second person and expires within hours; the vendor's staff are named in the contract; and the operator can cut every vendor connection from one control. NERC's low-impact standard CIP-003-9, in effect since April 1, 2026, requires registered entities with low-impact systems to have methods to determine vendor electronic remote access, to disable it, and to detect known or suspected malicious communications over it, as NERC's regional entities summarize the standard (ReliabilityFirst; MRO).

Monitoring. Passive monitoring of IEC 61850, DNP3, Modbus and BACnet traffic is already required. It should alert on four things in particular: write commands from an unexpected source, controller mode changes, program or firmware downloads, and new connections between zones. Independent metering at the 230 kV and 34.5 kV buses, read by a system outside the control zones, gives operators a check on what the controllers report.

Cooling. Each CDU and each heat-rejection unit keeps running on its local controller, closing its own loop on local sensors, when the BMS is unreachable, with a safe fallback setpoint if the last supervisory setpoint is stale; the fallback is tested at commissioning. The BMS supervises. It does not close the control loop. DCIM reads and does not command. Racks above 100 kW leave little time after loss of coolant flow, and the thermal study the design paper requires sets that time. The chiller-controller and building-framework flaws in Section 3 are the nearest evidence of risk to this plant.

Recovery. The Polish attack disabled devices that could not be restored remotely. The campus holds configured spares for remote terminal units, relays, gateways and controllers. It keeps firmware and configuration images offline and signed. A procedure to start, island and reconnect the campus by local control, with networks disconnected, is tested each year with the black-start test.

Coordination with the utility and the grid operator. NERC's May 2026 Level 3 alert is addressed to planning and operating entities, including transmission operators, reliability coordinators and balancing authorities, not to data center owners. It asks them to establish communication with the operators of computational loads, by voice or other means (NERC). The campus should also give Dominion and PJM three things they do not ask for today: its transfer and ride-through settings; notice before those settings change; and a tested way to confirm by voice any instruction received over a data link.

Whether NERC's cyber standards apply. This is an inference from the definitions, not a NERC determination. Generating resources connected at 100 kV or above fall within the Bulk Electric System where an individual unit's gross nameplate rating exceeds 20 MVA or the plant's aggregate rating exceeds 75 MVA. Generation is excluded if it sits on the customer's side of the retail meter and serves the retail

load, its net capacity provided to the system does not exceed 75 MVA, and standby, back-up and maintenance power is provided by a balancing authority or under a binding obligation (NERC BES definition). A campus whose generation sits behind its retail meter and whose net capacity to the system never exceeds 75 MVA can argue for the exclusion. One that exports more, or commits capacity it may export, likely cannot. The answer turns on the one-line diagram, the metering point and a registration assessment, not on this reading. If the engines and battery are in, they would not meet the 1,500 MW generation criterion for medium impact, but impact also depends on the other criteria of CIP-002, including any transmission facilities and control centers. Low impact is likely, not certain (NERC guidance). Low impact brings CIP-003 and little else. The design paper advised a CIP-equivalent baseline. This paper makes that specific: build the three level 4 zones to the requirements NERC sets for medium-impact systems, including internal network monitoring under CIP-015, whether or not registration requires it.

7 The compute platform

The server platform should be bought and run so that its firmware can be measured, its management controllers cannot be reached by tenants or the internet, and no claim made to a tenant depends on confidential computing alone. This section applies where the operator owns or manages servers. For a pure colocation hall, the parts on physical access and tenant audit apply.

Management controllers. A BMC can power, reimage and reflash a server regardless of its operating system. NSA and CISA advise hardening BMC credentials, updating BMC firmware, monitoring its integrity and isolating its network (NSA, June 2023). CISA's directive on management interfaces names out-of-band server interfaces such as iLO and iDRAC and gives federal agencies 14 days to remove an exposed interface from the internet or place it behind a separate enforcement point (CISA BOD 23-02). The 2026 record shows the exposure is current. An OpenBMC authentication bypass was published on September 15, 2026, and its record names NVIDIA among downstream users of the affected component; whether a given product is affected must be checked against its firmware (CVE-2026-16141). An HPE iLO 7 flaw rated 9.0 was published on October 5, 2026 (CVE-2026-79820). Campus rules:

- The BMC network is physically separate, has no route from tenant networks or the internet, and is entered only through the administrator access system in Section 8.
- Each BMC has unique credentials. Host-side management interfaces are restricted where the firmware allows it.
- Power, reimage and firmware commands that affect more than a set number of servers need approval by a second person and are rate-limited by the management system.
- BMC firmware is on the same patch schedule as the network edge.

Root of trust and firmware recovery. NIST SP 800-193 is the reference. It calls for platform firmware to be protected from unauthorized change, for changes to be detected, and for recovery to a known good state (NIST). The state of the art in 2026 is an open silicon root of trust (Caliptra), device attestation over

the DMTF SPDM protocol, and independent firmware review under the Open Compute Project's S.A.F.E. program. Three facts set expectations.

- Adoption is early. On October 11, 2026 the Caliptra registry of audited products listed two, both from NVIDIA and both on hardware revision 1.1, which accelerates LMS hash-based signatures in hardware, with ML-DSA on that revision a firmware feature (Caliptra registry; Caliptra README).
- The root of trust has had flaws of its own. A 2026 flaw in Caliptra's read-only code allows a secure-boot bypass in which attestation continues to report the originally verified image (CVE-2026-11835). Read-only code in fabricated chips cannot be patched.
- Independent review is available as procurement evidence. The S.A.F.E. repository held 147 published review reports across 21 vendor folders on October 8, 2026, covering server processors, GPUs, network cards, BMC firmware and drives (OCP S.A.F.E.).

Procurement terms that follow: firmware protection, detection and recovery to SP 800-193 for every device class in the server that supports it, including BMC, network card, GPU and drive, recorded in an acceptance matrix that lists for each device what is measured, the root of trust, the recovery authority and what cannot be recovered; attestation the operator can query; a published independent firmware review where one exists, with exceptions recorded; and signature schemes that will remain acceptable after 2030 (Section 8). Attestation is evidence. It is not proof.

Trust anchors expire. Microsoft's 2011 Secure Boot certificates began expiring in 2026. The key-exchange certificate expired on June 24, the third-party certificate on June 27, and the Windows boot manager certificate expired on October 19, 2026 (CVE-2026-21265). Microsoft says the certificates must be updated before expiry to keep receiving boot security updates, and that Windows Server does not receive the new certificates automatically (Microsoft). Red Hat notes that the update changes a measured-boot value, so secrets sealed to the old value must be resealed first (Red Hat). The operating requirement is an inventory of every trust anchor in firmware, with an owner and an expiry date.

Acceptance testing. NSA recommends acceptance testing at receipt to confirm that devices arrive untampered, with the expected hardware and firmware, and recommends devices with a TPM, UEFI Secure Boot and a Trusted Computing Group platform certificate (NSA guidance). NSA describes its own validation tool as a proof of concept not intended for production (NSA HIRS), so an operator must build this capability. Acceptance testing of this kind detects changes to measured firmware and, where components carry identities enrolled in the platform certificate, substitution of those components. It does not detect a device added to the memory bus, which is the subject of the next paragraph.

Confidential computing and its limit. AMD SEV-SNP, Intel TDX and NVIDIA GPU confidential computing protect a tenant's data in use against a compromised or untrusted host software stack. They are worth deploying for that purpose. On the processor generations and memory types tested, they have not withstood the published attacks by a party with physical access to the server.

Attack	Published	Requires	Defeats	Vendor response
BadRAM	Dec. 2024	Change to a memory module's configuration chip; less than $10 of equipment, or root access where the chip is not write-locked	SEV-SNP memory integrity and attestation	Firmware check added (AMD CVE record)
WireTap	Sept.–Oct. 2025	Physical access; passive DDR4 device under $1,000	SGX attestation key	Outside threat model (SecurityWeek)
Battering RAM	Sept.–Oct. 2025	Brief physical access; DDR4 device under $50	SGX memory confidentiality; SEV-SNP attestation	No mitigation planned (AMD-SB-3024)
TEE.fail	Oct. 2025	Physical access and host control; DDR5 device under $1,000	TDX and SGX attestation keys; SEV-SNP secrets; NVIDIA GPU attestation in a deployed system	AMD: no mitigation planned (AMD-SB-3040); Intel: earlier out-of-scope position unchanged (Intel)
DDRop	Sept. 2026	Host control and brief physical access; DDR5 device, parts under $200 per the authors	Integrity of TDX, SGX and SEV-SNP memory; forged TDX attestation	No CVE; AMD: no mitigation (AMD-SB-3048); Intel: evaluating hardening options, none issued (Intel)

The cost, access and effect entries were checked against the researchers' own project pages (BadRAM; WireTap; Battering RAM; TEE.fail; DDRop); the host-control requirement for TEE.fail rests on a press report of the research (BleepingComputer). The TEE.fail work reached GPU attestation by relaying attestation through the compromised processor environment, not by attacking the GPU itself. The vendor responses are from the vendors' own bulletins.

AMD's statement on TEE.fail is direct: it does not plan mitigations because physical attacks are out of scope for SEV-SNP. Intel advises operators to restrict and monitor physical access to servers. The consequences depend on the adversary.

- Against a remote intruder or a compromised host without physical access, four of the five attacks do not apply as demonstrated. BadRAM is the exception: where a memory module's configuration chip is not write-locked, an attacker with root on the host can carry it out in software, and AMD's firmware check is the mitigation. The exposure that remains is implementation flaws, which were numerous in 2025–2026 and are addressed by firmware updates where the vendor issues them.
- Against the facility operator, an insider or a maintenance contractor, it raises cost and removes software-only methods. It does not close the exposure. Forged attestation means the tenant cannot detect the compromise from attestation alone.
- Against an interdictor, a device can be fitted before delivery. The Battering RAM authors name supply actors as realistic attackers (Dark Reading).

The controls are therefore physical, and they are what a colocation operator can offer a tenant in a form the tenant can audit: two people present for any hands-on work on tenant servers; video and a written record of each such event; tamper-evident seals on chassis; inspection of memory slots at receipt and after maintenance; and custody records for memory modules and servers from the dock to the rack. The Cloud Security Alliance's guidance after DDRop is to treat attestation as strong evidence against remote and logical compromise and not as a substitute for physical security (CSA, Sept. 2026).

Isolation between tenants. Containers should not be the only boundary between GPU tenants. The NVIDIA Container Toolkit had three flaws between September 2024 and July 2025 that let a container reach the host or run code with elevated permissions, and a fourth, a race condition allowing code execution and privilege escalation, on June 30, 2026: CVE-2026-24260, rated 8.5. The boundary should be a virtual machine or a whole server per tenant. The high-speed fabric is part of the boundary. NVIDIA's UFM Enterprise fabric management software had an improper-authentication flaw in its web interface, CVE-2026-24170, rated 8.8, in August 2026 (NVIDIA bulletin). In NVIDIA's multi-GPU protected mode, traffic between GPUs is not encrypted and all GPUs must belong to one tenant (NVIDIA).

Returning a server to service for a new tenant. The procedure, drawn from the sources above:

1. Cryptographically erase every drive, verify the result and keep a record for each device.
2. Measure BMC, boot, network card, GPU and switch firmware against signed reference values, and reflash anything that differs or cannot be measured.
3. Export BMC logs to the protected log store, then reset BMC credentials and clear BMC storage.
4. Reset GPUs and clear device memory and any device-local keys by the vendor's documented procedure where one exists, verify the result, and record in the acceptance matrix what evidence of clearing the device can give and what residual state cannot be verified.
5. Record the attestation evidence before the server is assigned.

NIST finalized Revision 2 of its media sanitization guideline on September 26, 2025 (NIST SP 800-88 Rev. 2). Cryptographic erase relies on drive firmware. Until drives with attestable erase are in service, media leaving the site for a government tenant should be destroyed unless the tenant's standard says otherwise.

8 Network, identity and cryptography

The network edge and the administrator's identity are where the documented intrusions begin. The controls in this section are the ones with the most evidence behind them.

The edge.

- No management interface of any device is reachable from the internet. CISA's directive gives the two acceptable arrangements: an isolated management network, or an enforcement point separate from the device (CISA BOD 23-02).
- No edge device runs past its vendor's end of support. CISA ordered federal agencies on February 5, 2026 to inventory such devices within three months, remove listed devices by twelve months and all unsupported edge devices by eighteen months, and maintain continuous discovery by twenty-four months. CISA and its partners urged all organizations to follow it (joint fact sheet). The directive itself is cited here through secondary sources (Cisco summary; BleepingComputer).
- Remote administration does not rely on an internet-facing VPN gateway as its only control. A 2024 joint guide counted more than 22 exploited flaws related to VPN compromise and recommends moving to zero trust access services (CISA and partners).

- Edge devices are bought to the forensic logging specification the UK National Cyber Security Centre published for makers of network devices, which CISA and its partners endorse, and the campus forwards their logs off the device (CISA summary).
- Device integrity is checked against the vendor's image on a schedule, and after any exploited-flaw notice. A device that fails, or that was exposed while a flaw was being exploited, is replaced or rebuilt, and its credentials are rotated.

Zero trust on the management planes. NIST SP 800-207 gives the tenets: no trust from network location, access granted per session, and authorization enforced before every access (NIST). It also warns that the policy decision system becomes a target. On a campus this means the out-of-band network, the orchestration control plane, DCIM and the physical access system are each in their own segment, each reached only through the administrator access system, and the access system itself is protected and monitored as the most valuable asset on site. NSA's implementation guidelines of January 2026 define 91 activities for the target level and are a detailed public checklist (NSA primer; NSA release). NSA's zero trust guidance for control systems of October 8, 2026 selects 26 of the 84 activities in the Department of War's control-system guidance as high-impact steps that can be taken now: secure remote access, hardened controllers, visibility and micro-segmentation. It calls for vendor access through controlled gateways or privileged-access systems with session recording, and for a security broker, enclave, gateway or tunnel where a control protocol cannot be encrypted (NSA, Oct. 2026). It does not mention one-way gateways; the paper's use of them for the three highest zones goes beyond it.

Administrator identity.

- Authentication at NIST's highest assurance level. SP 800-63B-4 requires, at that level, a cryptographic authenticator with a non-exportable private key that resists phishing. It excludes passkeys that synchronize between devices. It caps a session at 12 hours and recommends a 15-minute inactivity limit (NIST SP 800-63B-4).
- Dedicated administration workstations that do nothing else, and no standing privilege. Rights are granted for a task and expire.
- Sessions bound to the device. Multifactor authentication protects the login and not the session token that follows. Proof-of-possession or certificate-bound tokens, where the identity system supports them, and short sessions address token theft.
- Two-person approval for commands that are irreversible or site-wide: firmware pushes, bulk power actions, deletion of backups or logs, changes to the access system itself. NIST's control for this is dual authorization, and NIST notes that organizations consider the risk of dual authorization where an immediate response is needed for public or environmental safety (NIST SP 800-53, AC-3(2)). Emergency accounts cover that case. Each use raises an alarm and is reviewed.
- Signing keys and certificate authority keys held in hardware security modules, with planned rotation. The Storm-0558 intrusion used a signing key created in 2016, and the review board reported that Microsoft did not know how or when the actor obtained it (CSRB). NSA's rules for commercial solutions

protecting classified data require hardware modules for online certificate authority keys and list two-person integrity for their administration (NSA CSfC annex).

- Identity proofing in person for staff who will hold privileged access. Mandiant reports North Korean remote IT-worker cases as a distinct category of intrusion with a median dwell of 122 days (M-Trends 2026).

Volumetric attack and routing. The largest attack Cloudflare has reported is 31.4 Tbps lasting 35 seconds. Cloudflare counted 935 network-layer attacks above 1 Tbps in the first half of 2026 and states that a 100 Gbps attack can take most unprotected data centers offline (Cloudflare Q4 2025; Cloudflare H1 2026). A campus should not plan to absorb an attack of that size on its own links, and 35 seconds is too short for a human decision. Mitigation is contracted upstream and is automatic. For routing, the campus publishes route origin authorizations for its own address space and requires origin validation from its carriers by contract, as the White House routing plan of 2024 recommends for all network operators (ONCD). Origin validation does not stop every form of route hijack, so prefix limits and route filtering remain necessary.

Post-quantum cryptography. Traffic recorded today can be decrypted later if its key exchange is broken by a future quantum computer. Data that must stay secret for many years is exposed now. The federal dates are set.

Date	Requirement	Source
August 13, 2024	NIST publishes FIPS 203, the ML-KEM key-establishment standard. FIPS 204 and 205 are the companion signature standards	NIST
2025–2033	NSA's CNSA 2.0 schedule for national security systems: firmware signing and traditional networking equipment exclusively by 2030; operating systems, web and cloud services by 2033	NSA FAQ v2.0, April 2024
2027	All new commercial national security systems must be able to support quantum-resistant algorithms; systems that cannot are to be phased out by 2030	NSA, Oct. 1, 2026
December 31, 2030	Federal high-value and high-impact systems use post-quantum key establishment. The order directs the federal acquisition council to propose a rule requiring covered contractors to comply with NIST's cryptographic standards by the same date	Executive Order 14412, June 22, 2026
December 31, 2031	The same federal systems use post-quantum digital signatures	Executive Order 14412
After 2030 and after 2035	NIST's draft plan: quantum-vulnerable public-key algorithms at 112-bit strength deprecated after 2030 and disallowed after 2035. The document was still a draft on NIST's site on October 22, 2026	NIST IR 8547 draft

Executive Order 14412 also directs CISA and NIST to publish minimum elements for a cryptographic bill of materials and directs sector agencies to help infrastructure owners plan their migration. It places no requirement on data center operators as such.

The software is ready for key establishment. OpenSSL has offered a hybrid post-quantum key share by default since version 3.5.0 in April 2025, and OpenSSH has used a hybrid ML-KEM exchange by default since version 10.0 in April 2025 and, from version 10.1, warns when a connection does not use a post-quantum scheme (OpenSSL; OpenSSH). Campus actions:

1. Inventory where public-key cryptography is used on the management planes, in firmware signing and on inter-building links.
2. Turn on hybrid post-quantum key establishment for TLS and SSH on management traffic wherever both ends support it, after compatibility testing. Keep strong classical configurations on BMCs and control-system devices that cannot yet support it, and record them in the inventory.
3. On point-to-point encrypted links between buildings and to nearby sites, use pre-shared symmetric keys of at least 256 bits for MACsec or IKEv2, the interim measure NSA specifies for classified traffic, with a unique key per link and a written procedure for distribution, rotation and recovery (NSA CSfC annex, March 2026).
4. Require that servers, network equipment and controllers bought now can verify firmware with a post-quantum or hash-based signature, since they will be in service after 2030.
5. Do not buy quantum key distribution. NSA does not recommend it for national security systems and regards post-quantum cryptography as the more cost-effective and maintainable solution (NSA).

9 Supply chain and software assurance

A campus is exposed through its suppliers in four ways, and each has a documented case. The design paper named firmware supply and vendor access as its largest residual risks. This section sets the controls.

Exposure	Case	Control
Software or firmware altered before delivery	SolarWinds; the XZ Utils backdoor, included in two releases of a legitimate open-source project (NVD)	Signed artifacts verified at install; provenance for anything built in-house; dependency review; staged deployment with behavior monitoring, since a compromised build or signer produces validly signed code
A service provider's access used against its customers	Silk Typhoon's use of stolen provider keys; Google's assessment that BRICKSTORM operators target service providers to reach their customers	Brokered access; named personnel; provider credentials treated as the operator's own
Updates altered in transit	An internet service provider compromised to falsify update lookups	Signature verification independent of the network; pinned update sources

Exposure	Case	Control
Theft of a vendor's source code and vulnerability information	F5, October 2025	Assume unpublished flaws exist in the product; reduce reachability; watch for vendor breach notices

Software the operator builds or deploys. The SLSA framework's current specification is version 1.2. Its build levels run from provenance that shows how a package was built, to signed provenance from a hosted build service, to a hardened and isolated build service (SLSA v1.2; SLSA build track). The proposed rule for a campus: the second level for all management software, and the third for anything able to push code or firmware to every server or controller. NIST's control catalog supplies the install-time requirement, which is to prevent installation of software and firmware that is not signed with an approved certificate (NIST SP 800-53, CM-14). Build systems should have no general outbound internet access.

Vendor obligations that now exist. The European Union's Cyber Resilience Act began to apply its vulnerability and incident reporting obligations to manufacturers on September 11, 2026, with full application on December 11, 2027, according to the Eclipse Foundation's summary of Article 71 (Eclipse ORC). Vendors selling in Europe will have reporting processes a U.S. buyer can ask to be included in.

Servers and components. Section 7 gave the terms: measured and recoverable firmware, a published independent firmware review, acceptance testing at receipt, and physical inspection. One design feature matters for interdiction. In the Caliptra design the owner programs fresh secret material at first use, so that a device secret stolen at the factory cannot be used to impersonate the part afterward (Caliptra specification).

Power equipment. Three federal actions affect procurement for the battery and any inverter-based equipment.

- The Federal Communications Commission's July 28, 2026 notice adds foreign-produced power inverters to its Covered List, which blocks authorization of new models unless the Department of War or the Department of Homeland Security grants a conditional approval (FCC DA 26-786). A second notice of August 20, 2026, issued after a further Department of War determination, defines a covered inverter as a grid-tied, utility-interactive device that contains or is configured to accept a remote-communication component, wired or wireless, including Ethernet (FCC DA 26-870). Wired-only communication therefore does not take an inverter outside the listing. The same notice redefined foreign-produced: an inverter eligible for the domestic-production credit under 26 U.S.C. § 45X, or qualifying as a domestic end product under 48 CFR 25.101(a) with domestic components above 65% of component cost for deliveries through 2028 and 75% from 2029, is outside the listing. Neither notice names battery power conversion systems; whether a grid-tied battery converter is covered is a question for counsel. The FCC states that the listing does not prohibit the import, sale or use of existing models (FCC fact sheet), and a waiver permits software and firmware updates to devices authorized

before July 28, 2026 until at least January 1, 2029 (FCC DA 26-789). Earlier law-firm readings that wired-only equipment might fall outside the listing predate the August notice (K&L Gates).

- The fiscal year 2026 defense authorization act, Public Law 119-60, restricts what the Department of Defense buys. Section 847 bars the use of fiscal year 2026 funds to contract for photovoltaic cells, modules or inverters manufactured by a foreign entity of concern; it applies only to direct departmental procurement, not to third-party financing arrangements; the Secretary may waive it after determining that no alternative source exists and that there is no national security risk, with written certification to the defense committees 30 days before contracting; assets that enhance combat capability get a one-year delay; and intelligence, electronic warfare and information warfare activities are exempt. Section 842 adds 10 U.S.C. 4865, which requires advanced batteries and cells whose functional cell components and technology are not owned, sourced, refined or produced from a foreign entity of concern, applying to new acquisition programs on January 1, 2028, standard batteries on January 1, 2029 and existing programs on January 30, 2031, with exceptions and a one-year waiver (Pub. L. 119-60, §§ 842 and 847; summary: Baker McKenzie). Neither section reaches a commercial campus directly; whether a defense tenant's contract imposes either must be read from that contract.
- FERC Order No. 912 directs NERC to strengthen supply-chain standards for registered entities, including a maximum time between a supplier risk assessment and installation. FERC declined to require entities to validate the data vendors give them (FERC Order No. 912).

The evidence on inverters should be stated with care. The 2025 Reuters report was not confirmed by the Department of Energy's review as reported. The FCC's action rests on dependence, remote connectivity and a documented case of a manufacturer remotely disabling inverters in a commercial dispute, according to law-firm summaries (Squire Patton Boggs). The paper's control is the one in Section 6: no active wireless connectivity, by omission or by a manufacturer-supported disablement, and no vendor connection except through the access broker, verified at commissioning, whatever the origin.

Contract terms. For every supplier of control systems, management software and remote services:

- A software bill of materials and a list of every communication interface, documented and tested at acceptance.
- Signed firmware and a commitment to security updates for a stated number of years.
- Notice of any intrusion at the supplier within a stated number of hours.
- No remote access except through the operator's broker.
- For government tenants, Section 889 and Covered List checks, as the design paper requires.

Vendor concentration. Section 4 identified shared control products and shared remote access as the condition for a grid-scale event. An operator with several campuses should know which share a microgrid controller, a UPS family, a battery plant controller or a remote-service provider, and should require of those vendors the strongest terms above. A utility or grid operator could ask the same question across all large loads in its territory. No current rule asks it.

10 AI workloads and model weights

A campus that hosts frontier AI training or inference holds an asset for which RAND's framework assumes state operations lasting years and costing up to $1 billion: the model weights. No binding U.S. rule sets security requirements for a domestic data center because it hosts AI compute. The working reference is RAND's 2024 framework, and it places demands on the building, not only on the tenant's software.

The RAND framework. RAND identifies 38 attack methods in nine categories and defines five security levels against five classes of attacker (RAND RR-A2849-1). Level 3 is meant to defeat criminal groups and insiders. Level 4 is meant to defeat most standard operations by leading state institutions. Level 5 is a system that could plausibly be claimed to defeat most of their top-priority operations. RAND judges that defending an internet-connected system against the most capable actors is currently not feasible with off-the-shelf solutions and standard industry practice and that the measures needed may take about five years to develop. It rates supply attacks through equipment and services among the most feasible methods for the two highest attacker classes. RAND gives no cost for any level. Its August 2026 follow-on report turns level 3 into 262 controls adapted from NIST SP 800-53, addressing 31 high-feasibility attack methods, for implementation in six to twelve months (RAND RR-A4704-1).

What each level asks of the facility. The level 3 and 4 entries are RAND's benchmark measures as they bear on a building. The right-hand column is the author's reading for a colocation or build-to-suit operator.

Level	Facility measures in RAND's benchmark	What the operator must be able to deliver
3	Data centers guarded or locked at all times; premises checked for intruders and unauthorized devices; security-minded hardware sourcing; integrity checks against a reference image	A standard high-security hall with documented sweeps, sourcing records and firmware measurement
4	Isolation of weight storage; hardware-enforced limits on output rate; reduced communication capability; more guarding; logging of all access; devices prohibited near the systems; hardware audited and validated; an advanced insider-threat program; protection against eavesdropping and the simplest emanation attacks	A separate enclave for weight storage and use, with its own network, a device-free zone, two-person entry and a physical limit on outbound data rate. RAND notes this may require changes to how data centers are set up
5	Completely isolated network for weight storage; formal hardware verification of key components; advanced side-channel defenses	Not attainable for a service that must answer the internet with current commercial practice, on RAND's judgment. An isolated research enclave is the nearest case

Confidential computing is not the control for this adversary. RAND lists confidential computing at level 4 with the qualifier "when available." The attacks in Section 7 show why it cannot be the main protection against an actor with physical access. GPU confidential computing depends on the processor's protected environment. When researchers extracted processor attestation keys in the TEE.fail work, they bypassed GPU attestation in a deployed system as well. Confidential computing remains useful against software-level access by operator staff and against a remote intruder.

The software around the accelerators. Section 7 covered the container and fabric flaws. For weight protection the consequence is that a tenant sharing a cluster with other tenants by containers alone should treat escape through a vulnerable toolkit or driver as a realistic means of reaching the host and then other tenants' memory. Single-tenant clusters, or virtual-machine isolation with dedicated fabric partitions, are the conservative choice.

Policy in formation. Four items could become requirements. None is one today.

- The July 2025 AI Action Plan calls for new technical standards for high-security AI data centers, led by the Department of Defense, the intelligence community, the National Security Council and NIST, and for an AI information sharing and analysis center led by the Department of Homeland Security (White House). NIST and its Center for AI Standards and Innovation issued a draft in July 2026, SP 800-239, which covers the computing environment and places the building, the perimeter and the power and cooling control systems out of scope; comments closed September 25, 2026 (NIST SP 800-239 ipd). No standard for the facility itself was found, and the information sharing center had not been established as of February 2026, when a CISA official said there was no timeline for it (Cybersecurity Dive); no later announcement was found by October 23, 2026.
- Section 1513 of the fiscal year 2026 defense authorization act directs the Department of Defense to write a cyber and physical security framework for the AI systems it acquires, whose covered technology includes model weights, with its most stringent tier to give protection similar to that of national security systems, and to apply it through an amendment to the defense acquisition regulation supplement or similar action. The covered entities are those that enter a contract or other agreement with the Department under which they develop, deploy, store or host such systems. A data center operator with such an agreement would be covered; one hosting a defense contractor's workload without its own agreement with the Department is not reached by the statute itself, and any obligation would come from the implementing acquisition rule and the contractor's terms (Pub. L. 119-60, § 1513; Crowell & Moring). No published framework or acquisition rule was found by October 23, 2026.
- The March 2026 national cyber strategy says the government will secure the AI technology stack, including data centers (White House). It sets no requirement.
- The Commerce Department's Data Center Validated End User program, which applies to approved foreign sites, is the one U.S. instrument with written security conditions for AI data centers. Applicants describe physical and logical security for each location and supply an information security plan, a personnel security plan and a supply plan that keeps PRC-origin equipment out of the data center (89 FR 80080). It is a reasonable indication of what a domestic standard would ask.

Design position. A campus built for frontier AI tenants should include at least one hall built to the facility measures of RAND's level 4: separate structure or separately secured wing, its own network with a hardware limit on outbound data rate, a device-free zone, two-person entry, and custody controls on every component entering it. The building alone does not make a tenant level 4; weight handling, host security and insider controls remain the tenant's. The operator should say plainly to tenants that RAND

judges level 5 not currently feasible for an internet-connected system using off-the-shelf solutions and standard industry practice, and why. No public cost estimate for these levels was found.

11 Detection, response and recovery

The adversary in Section 3 uses valid credentials and the system's own tools, on devices that cannot run endpoint detection, for a year or more. Detection has to be built for that case.

Detection.

- Retain logs from the edge, the identity system and the management planes for 24 months in a searchable form. That figure is the author's choice. It exceeds the 393-day average and the 17-month government-documented case. It does not cover the three- and five-year cases, for which archived logs are the only recourse.
- Store logs on a separate system, protect their integrity cryptographically, and require two people to move or delete them. These are NIST controls AU-9(2), AU-9(3) and AU-9(5) (NIST SP 800-53).
- Watch the network around devices that cannot be instrumented. Management-network traffic from BMCs, switches, firewalls, power distribution units and DCIM gateways is regular. New destinations, new protocols and outbound connections are the signals.
- Watch administrator behavior. Every privileged session is recorded. Bulk actions, access outside a change window and first-time access to a system are reviewed by a person.
- Place decoys. MITRE's defensive catalog defines decoy credentials and decoy session tokens (MITRE D3FEND, decoy user credential; decoy session token). Use of a decoy administrator credential is a high-priority alarm to be investigated at once. Authorized testing, sanctioned automation and deployment error are the innocent explanations, and procedure can account for them. This is one of the few detections that works against an intruder using valid credentials.
- Verify device integrity on a schedule: edge appliances against the vendor's image, server firmware by attestation, controller programs against the offline reference copy.
- Use government indicators when they are issued. The BRICKSTORM report includes detection rules and was updated twice in December 2025.

Mandiant found that organizations first detected the intrusion themselves in 52% of its 2025 investigations, up from 43% (M-Trends 2026). Dragos reports ransomware in control environments found in an average of 5 days where monitoring was comprehensive, against 42 days overall. That is a vendor's figure (Dragos).

Response. Removing a state actor from the management planes means rebuilding identity. The plan, written before it is needed, covers:

1. Isolation of the affected management plane while power and cooling continue under local control.

2. Rotation of every credential, token and signing key the actor could have reached, including federation keys and the keys held by appliances.
3. Rebuild of affected systems from known-good images. Edge appliances with firmware-level persistence are replaced.
4. A decision rule on tenant notification, agreed with tenants in advance.

CISA maintains a public tool that maps observed adversary techniques to containment and eviction steps and is suited to planning exercises (CISA Eviction Strategies Tool).

Recovery. Backups, reference images and emergency credentials are held under an administrative authority separate from production, so that one compromised identity cannot destroy both. NIST's controls call for backups stored separately, protected cryptographically, tested by restoration, and deletable only by two people (NIST SP 800-53, CP-9). For control systems, Section 6 set the requirements: configured spares, offline signed images and an exercised manual mode.

Exercises. Three scenarios test the principles in Section 5.

1. A management-plane intruder issues a power-off command to all servers through the BMC network. Does the two-person rule and the rate limit hold? How long to restore?
2. The microgrid controller receives an island command during a grid disturbance. Does the hardwired permissive hold? Can operators confirm the instruction with the utility by voice?
3. A memory-bus device is found in a tenant server during maintenance. Can custody records show when it was fitted and who had access?

Reporting and sharing. The legal position is unsettled in three respects.

- CISA's rule under the 2022 incident-reporting act is not final. The White House regulatory office's list of rules under review shows the final rule received on October 1, 2026 and still under review on October 22 (OIRA list; OIRA review page; trade report: Security.io). The 2024 proposal required a report within 72 hours (89 FR 23644).
- The liability protections of the Cybersecurity Information Sharing Act of 2015 lapsed on September 30, 2025 (DWT), were restored by short extensions (Hunton), and now expire on December 11, 2026 (Pub. L. 119-103, Div. B § 2011, approved September 2, 2026; CRS).
- No information sharing center specific to data centers was identified in this research. The operator's channels are CISA and the FBI, and the AI center the 2025 plan proposes, if it is established.

A registrant's duty to disclose a material incident to the Securities and Exchange Commission within four business days of determining materiality is unchanged. A defense contractor's incident-reporting clause, DFARS 252.204-7012, remains in force (Section 12).

Insurance. Lloyd's has required since March 31, 2023 that standalone cyber policies exclude losses from state-backed attacks that significantly impair a state's ability to function or its security capabilities, and that policies set out how an attack is to be attributed (Lloyd's Y5381). No 2025–2026 court decision

applying these clauses was found. The Merck decision of 2023 concerned older wording and settled before the state's highest court ruled, as law-firm and practice-guide summaries describe it (Simpson Thacher; Chambers). An operator should read its property and cyber policies against two cases: a quiet espionage intrusion, and a destructive attack that is part of a wider campaign. The second is the one the exclusion was written for.

12 Law, regulation and standards

No federal statute or rule imposes cybersecurity requirements on a U.S. data center because it is a data center. Obligations reach an operator in five other ways: its tenants' contracts, the electric reliability regime, securities law, the pending incident-reporting rule, and export-control conditions. The table gives the status of each instrument on October 23, 2026.

Instrument	Binding on a campus operator?	Status and trigger	Source
Critical infrastructure sector status	No direct duty	No sector names data centers. The Information Technology Sector, with the Department of Homeland Security as its agency, covers hardware, software and service providers, and the Congressional Research Service lists no data center sector. A March 2025 executive order, EO 14239, directed a review of all critical infrastructure policies, naming the 2024 memorandum NSM-22; CRS reported in March 2026 that it could not find the resulting documents. Executive Order 14412 of June 2026 still cites NSM-22	CRS R48878; EO 14239; EO 14412
National cyber strategy, March 6, 2026	No	Names data centers under two of its six pillars. Sets no requirement. Its second pillar is to reduce regulatory burden	White House
Federal incident reporting (CIRCIA)	Not yet	Proposed April 4, 2024. Final rule received for White House review on October 1, 2026 and still listed as under review on October 22. Under the proposal, an entity in a critical infrastructure sector above the small-business size standard, or one meeting a sector-based criterion such as knowingly providing IT hardware, software, systems or services to the federal government, would be covered	89 FR 23644; OIRA list; OIRA review page; Security.io
SEC Form 8-K Item 1.05	If the operator is a registrant	In force. Industry groups have asked the Commission to rescind it; only a request for comment is open	SEC adopting release, 88 FR 51896; 17 CFR 249.308; CTIA letter

Instrument	Binding on a campus operator?	Status and trigger	Source
NERC CIP standards	Only if the campus holds a registered function and has bulk electric system cyber systems	See Section 6. Impact set by the CIP-002 criteria; low impact likely for onsite generation, not assured	NERC BES definition; CIP-002 guide
NERC registration of computational loads	Proposed	FERC's July 16, 2026 order requires NERC to file standards and registration criteria by December 31, 2026. NERC's registration criteria, revisions to its Rules of Procedure that its Board approved and that NERC filed with FERC on October 21, 2026, would register sites of 50 MW or more supplied at 100 kV or more, pending FERC approval (NERC Large Loads Action Plan). The draft standards cover modeling data, operating data and communications, and protection coordination. NERC's August slides list no cyber security requirement and record that a separate security request was referred to its Security Working Group (NERC slides, Aug. 2026). All three passed initial ballot in September 2026 (APPA, Sept. 2026) and final ballot, which closed on October 14, 2026 (APPA, Oct. 15, 2026); NERC's project page records final-ballot weighted segment approval of 82.3%, 78.1% and 82.7% for CLO-001-1, CLO-002-1 and CLO-003-1, against 81.6%, 77.9% and 82.4% in the initial ballot (NERC Project 2026-02); an ERCOT presentation of October 15 reports a special Board of Trustees meeting planned for late October or early November and filing with FERC by the end of the year (ERCOT presentation, Oct. 15, 2026). The texts, read in their first and final-ballot postings, contain only the secure-transfer clause described below	FERC RD26-7-000; NERC bulletin; Texas RE
NERC reliability guideline on large loads, May 2026	No	Non-binding. Its seventh chapter asks registered entities and large-load owners to segment the load's control networks from its IT networks, to use encrypted and authenticated protocols for all data exchange, to control remote access to systems that could affect the grid, to vet control-system suppliers, to assess and patch vulnerabilities, and to write joint incident response plans into the interconnection agreement. It aligns these with CIP-014, CIP-005, CIP-007, CIP-013 and CIP-008	NERC guideline, April 2026 text

Instrument	Binding on a campus operator?	Status and trigger	Source
CMMC	By tenant contract	A memorandum announced July 13, 2026 suspended Level 2 third-party and Level 3 assessments, the program's second phase, pending a 60-day review. Phase 1 self-assessments and affirmations continue where contracted. The reform task force's report was due to the department's chief information officer on September 11, 2026 ; a law firm reported on September 21 that it had not been made public (Covington), and no public version was found by October 23. The 252.204-7012 clause and NIST SP 800-171 Revision 2 remain. Under the rule, a provider that handles neither controlled unclassified information nor security protection data is not an external service provider	DoD CIO, CMMC; Latham & Watkins; 32 CFR 170.4; 32 CFR 170.19
NIST SP 800-172 Revision 3	By contract, when adopted	Final May 13, 2026. Enhanced requirements for protecting controlled unclassified information in critical programs and high-value assets. A vendor source reports that the department's Level 3 still references the 2021 edition	NIST
DoD cloud security requirements	On the cloud provider; passed to the landlord as build requirements	Impact Level 5 requires physical separation from non-federal tenants. Level 6 requires dedicated infrastructure and a facility clearance	CSP SRG V1R2
ITAR, 22 CFR 120.54	Paragraphs (a)(5) and (b) define when sending or storing encrypted technical data is not an export, reexport or retransfer	Sending or storing unclassified technical data secured by end-to-end encryption is not an export only if every condition of § 120.54(a)(5) and (b) is met: the data stays encrypted between originator and intended recipient with no means of decryption given to a third party; the cryptography uses FIPS 140-2 modules or their successors, supplemented by implementation, key-management and procedural controls consistent with NIST guidance, or other means at least comparable to AES-128; the data is not intentionally sent to or stored in a country proscribed under § 126.1 and is not sent from one; and the intended recipient is the originator, a U.S. person in the United States or a person otherwise authorized to receive it	eCFR
Export controls on AI compute	No domestic security requirement	The January 2025 diffusion rule is unenforced but, per the Government Accountability Office in May 2026, legally in effect until its rescission is completed. No replacement is published	GAO B-337935
Executive Order 14412 on post-quantum cryptography	Federal systems; contractors by a rule to be proposed	See Section 8	White House

Instrument	Binding on a campus operator?	Status and trigger	Source
FCC Covered List	On equipment authorization	Affects what inverters can be bought new. See Section 9	FCC
TSA pipeline security directives	On the pipeline operator	Reach the campus only through its gas supply contract; the TSA page lists the directives without stating their scope	TSA
Virginia Code § 18.2-186.6	Narrowly	Breach notification where the operator maintains personal information. No Virginia statute on data center cybersecurity was found	Va. Code § 18.2-186.6; Virginia Attorney General

The gap in the electric regime. The standards NERC is drafting would, if adopted, make a 50 MW data center supplied at 100 kV or above a registered entity with duties to supply data, maintain communications with the grid operator and coordinate protection. The three drafts were read for this paper in their first formal posting and in the final-ballot text of October 2026, balloted October 9–14: CLO-001-1 on interconnection, studies and modeling data, CLO-002-1 on operational data and communications, and CLO-003-1 on protection coordination and disturbance monitoring (first posting: CLO-001-1; CLO-002-1; CLO-003-1; final ballot: CLO-001-1; CLO-002-1; CLO-003-1; final ballot announcement). They create new data and communication links between the campus and the grid operator. In both versions CLO-002-1 requires the data specification of each transmission operator, balancing authority and reliability coordinator (requirements R1.3.6, R2.3.6 and R3.3.6) to include “mutually agreeable method(s) for securely transferring data and information” and sets no other security requirement; CLO-001-1 and CLO-003-1 contain none; and none of the three addresses the load-control functions behind the links. NERC’s cyber standards apply to listed functional entities, and the proposed computational load owner and operator are not on that list. The civil penalty authority for reliability standards is about $1.58 million per violation per day, as a law firm reports it (Willkie). The authority exists. The cyber requirement does not.

Colocation and tenant compliance. The design paper explained that a tenant handling controlled unclassified information inherits the landlord’s physical protection controls and needs a shared-responsibility matrix. Two additions. First, the landlord’s badge, video and visitor systems that protect a tenant’s enclosure are plausibly security protection assets within the tenant’s assessment, which is the practical way the defense program reaches a landlord. Second, with third-party assessment suspended, the regulatory requirement is unsettled, but prime contractors may continue to ask for evidence. An operator serving defense tenants should hold that evidence regardless.

Foreign comparators. Other governments regulate data centers by name.

- The United Kingdom designated data centres as critical national infrastructure on September 12, 2024 (UK government). Its Cyber Security and Resilience Bill, as amended in Grand Committee, was listed for report stage in the House of Lords on October 26, 2026, the sitting date still shown on October 23 (Report stage) (stages) (UK Parliament). The Bill covers data centres with a rated IT load of 1 MW or more, or 10 MW for enterprise sites, with Ofcom as regulator, incident notice within 24 hours and full notification within 72 (HL Bill 49). The same Bill would bring load controllers, organizations that remotely control energy smart appliances such as batteries and vehicle chargers with a combined capacity of 300 MW or more, within the network and information systems regime; a campus operating its own microgrid is not that category (UK factsheet). The energy department consulted from June to September 2026 on a cyber assessment framework for load controllers (DESNZ; also HSF Kramer).
- The European Union's implementing regulation under its NIS2 directive, in force since November 7, 2024, sets the technical measures for data centre service providers that fall within the directive's scope (Regulation (EU) 2024/2690) (Hunton). A compliance firm's summary says its annex of technical requirements includes environmental and physical security (Advisera).
- Singapore's 2024 amendment created a class of foundational digital infrastructure that names data centres, with codes of practice and incident reporting. Law firms report that these provisions had not been brought into force when other parts of the Act commenced in October 2025; that report is not linked here (CSA Singapore). A separate Digital Infrastructure Bill, consulted on from July 1 to 22, 2026 and introduced on September 8, 2026, would license major colocation and cloud data centres with a critical IT load of 10 MW or more for security and resilience, excluding facilities used only for the operator's own purposes, and would license every data centre with a critical IT load of 3 MW or more for energy efficiency (MDDI; Bill 20/2026). Parliament's record of bills shows the Bill passed on October 7, 2026, as a law firm also reports (Drew & Napier, Oct. 15, 2026; Parliament of Singapore; also W.Media).

A 100–300 MW campus would far exceed the UK and Singapore data centre thresholds; the EU regime turns on the operator's size and status under the directive and national law, not on its load. The UK's 300 MW load-controller regime is a separate category that a campus operating its own microgrid does not ordinarily fall within.

Voluntary baselines. The applicable documents are NIST SP 800-82 Revision 3 for control systems (NIST, Sept. 2023), ISA/IEC 62443, NIST SP 800-53 and SP 800-207, and CISA's Cross-Sector Cybersecurity Performance Goals, which trade press reports were reissued on December 11, 2025 with IT and control-system goals merged (Utility Dive). A guide led by Australia's signals directorate and co-sealed by CISA, NSA and the FBI gives six principles for control-system security. The first is that safety is paramount, and the fourth is to segment and segregate control systems from all other networks (ASD). The data center facility standards and audit reports that tenants usually ask for were not opened in this research and are not characterized here.

13 Cost and staffing by scale

The security program in this paper costs an estimated $9–14 million a year for a stand-alone 200 MW campus, about $4.50–7.00 per MWh of facility energy. That is the author's planning model, not a procurement estimate. It covers the cyber, control-system and technical-assurance program; it excludes physical guarding and the operation of a level 4 enclave, which are not priced here. Public benchmarks for a data center operator's security cost do not exist in the sources found, and public unit prices were found for almost none of the equipment.

What the public benchmarks say, and why they do not transfer.

- Enterprise security budgets averaged 10.9% of IT spending and 0.69% of revenue in 2025, in a survey of 587 chief information security officers. The 2026 edition reports the share of IT spending at 9.9% (IANS 2025; IANS 2026). These ratios describe corporate IT. In the author's judgment they usually leave out physical security, control-system security and secure construction.
- The Uptime Institute reports that 57% of operators' most recent major outages cost more than $100,000 and one in five cost more than $1 million (Uptime 2026). These are outage costs from all causes.
- The Department of Defense's estimate for implementing its Level 3 enhanced requirements is $2.7 million in one-time engineering for a small entity and $21.1 million for a larger one, with $0.49 million and $4.12 million a year in recurring cost, as vendors reproduce the rule's regulatory impact analysis, which this research could not read past its opening pages (89 FR 83092; Petronella). This is the only government estimate found for implementing enhanced requirements of this kind. It is per organization, not per facility.
- One trade report says accredited secure-facility construction frequently exceeds $500 per square foot (Bisnow).

Staffing model. The arithmetic is shown so it can be changed. One position staffed at all hours is 8,760 hours a year. At 2,080 paid hours per person that is 4.2 people. At 1,780 hours actually on shift, an assumption that allows for leave and training, it is 4.9. No authoritative published ratio was found; MITRE's guide to security operations centers contains none in the part this research could open.

Function	Staff	Basis
Security operations, two analysts on every shift, both trained for IT and control systems	8.4–9.8	2 positions × 4.2–4.9
Detection engineering and threat hunting	3	Author's estimate
Control-system security engineers	3	Author's estimate
Identity, keys and privileged access	2	Author's estimate

Function	Staff	Basis
Platform and firmware integrity	3	Author’s estimate
Vulnerability and supplier assurance	2	Author’s estimate
Incident response and forensics	2	Author’s estimate
Compliance and tenant assurance	2	Author’s estimate
Architecture and management	2	Author’s estimate
Total	**27.4–28.8 positions; 28–29 people**	

This is a campus run alone. An operator with several campuses shares most functions centrally. The author’s estimate for the staff who must be at or dedicated to each site is 10–12: the control-system engineers, a share of security operations, and platform integrity. A sector survey found that only 9% of respondents work full time on control-system security (SecurityWeek). A dedicated team of three is more than most asset owners have.

Annual cost.

Item	Low	High	Basis
Labor	$5.2 million	$7.25 million	28 staff at $185,000 to 29 staff at $250,000. Fewer than 28 people cannot fill 27.4 positions. The low rate is the federal median wage for information security analysts, $129,180 in May 2025, used as the wage proxy for all nine functions, times 1.43 for benefits. The high rate is the author’s allowance for seniority, shift pay and clearances
Tools and outside services	$4.0 million	$6.75 million	Author’s allowance: log storage and analysis, network monitoring for IT and control systems, privileged access and key management, annual adversary testing, firmware review, incident response retainer. No public prices were found
Total	**$9.2 million**	**$14.0 million**	

The benefits multiplier is from federal data: benefits were 30.0% of private-industry compensation in June 2026 (BLS). The wage figure is the Bureau of Labor Statistics median (BLS; also WageDex).

In proportion. The design paper's reference campus uses about 2,015 GWh a year, an average facility load of about 230 MW. The program therefore costs about $4.50–7.00 per MWh. Three comparisons from the design paper:

- The resilience premium of the recommended power configuration was about $23 per MWh, or $46 million a year. The security program is 20–30% of that.
- IT equipment for a 200 MW AI deployment is about $5 billion at the secondary figure the design paper used. The program is 0.2–0.3% of that value each year.
- Holding that equipment idle costs about $42 million a month. The annual program costs less than two weeks of that carrying cost.

Capital. The author's allowance for the security content of the build is $10–25 million: the separate management network, zone separation and one-way gateways, control-system monitoring, key-management hardware, administration workstations, the log platform and the commissioning tests in Section 6. That is $0.05–0.125 million per MW of IT, or 0.3–0.7% of facility construction at the design paper's $17.6 million per MW. It excludes a level 4 enclave for model weights and any accredited secure space. This figure is the least supported number in the paper. It should be replaced with vendor quotations.

By scale. The table is the author's judgment of what is proportionate.

Scale	Adversary to plan for	Security operations	Minimum measures
Edge, under 1 MW	Criminal and opportunistic; state actors through the network edge	Central, remote	No exposed management interface; no default accounts; BMC network isolated; supported edge devices only
Small enterprise, 1–5 MW	As above	Shared corporate team	As above, plus hardware-bound administrator authentication and off-site protected logs
Colocation, 10–50 MW	State actors for some tenants	Central, at all hours, across sites	As above, plus control-system zones with one-way transfer from protection, brokered vendor access, auditable physical controls on server work
Hyperscale and AI, 100–300 MW	State actors, including for grid effect	28–29 stand-alone, or 10–12 on site with central support	The configuration in Section 14
Gigawatt campus	As above; likely a registered entity	Dedicated	As above, plus a level 4 enclave, different control vendors between phases where practical, and standing coordination with the grid operator

The measures in the first two rows cost little. They are also the ones the record shows being missed: an exposed interface, a default account, an unsupported device.

14 Recommended configuration, implementation sequence and policy recommendations

For a 100–300 MW campus the recommended security configuration has twelve elements. Each answers a documented entry method or limits a documented consequence. None depends on knowing the adversary's technique in advance. Several are engineering controls whose effect at campus scale has not been tested; they are design requirements, not proven defenses.

#	Element	Answers	Section
1	No management interface reachable from the internet; no edge device past end of support; no remote administration that relies on an internet-facing VPN gateway as its only control	Edge-device entry	8
2	A physically separate management network for BMCs and infrastructure, with no route from tenants or the internet	Management-plane entry; site outage through BMCs	7
3	Hardware-bound administrator authentication, dedicated workstations, rights that expire, sessions bound to the device	Stolen credentials and tokens	8
4	Two-person approval and rate limits for irreversible or site-wide commands	One stolen identity; one insider	5, 7, 8
5	Signing and certificate authority keys in hardware modules, with rotation	Long-lived keys	8
6	A level 4 target for protection, power control and battery plant zones; one-way transfer out; untrusted treatment of utility and vendor links	Control-system entry; grid effect	6
7	Hardwired permissives for reconnection and commanded islanding; battery power and ramp limits enforced locally under separate write authority and backed by interconnection relays; setting changes at the device or under two-person control; mode switches in run	Consequence of a compromised control network	6
8	No default accounts and no active wireless modules at energization, verified as commissioning hold points	The Polish and 2026 controller attacks	6
9	Server and controller firmware that is signed, measurable and recoverable; acceptance testing and physical inspection at receipt	Firmware persistence; interdiction	7, 9
10	Auditable physical controls on hands-on server work, with a hall built to RAND level 4 facility measures available for model weights	Physical attacks on protected memory; weight theft	7, 10
11	24 months of protected logs; network monitoring around devices that cannot be instrumented; decoy credentials	Long dwell with valid credentials	11

#	Element	Answers	Section
12	Recovery images, spares, backups and emergency credentials under a separate authority; manual operation exercised yearly	Destructive attack	6, 11

Implementation sequence. Most of these elements cost little if decided at design and a great deal if added later. The sequence follows the project.

Project stage	Decisions and actions	Evidence to keep
Site and concept design	Zone plan and targets; separate management network; location of the weight enclave; which limits are hardwired	Zone and connection drawings; a list of engineered limits with the consequence each one bounds
Detailed design	Synchronism-check and islanding permissives; one-way gateways with a protocol-by-protocol interface list; independent metering; local autonomy of cooling loops; time-source analysis; protection coordination, short-circuit, ride-through, stability and load-rejection studies that include the hardwired limits	Design review records; time-loss and false-time analysis for each consumer
Procurement	Contract terms from Sections 7 and 9; post-quantum firmware signing; independent firmware reviews; Covered List and Section 889 checks	Supplier attestations; bills of materials; interface lists
Factory and site acceptance	Acceptance testing of servers; inspection of memory slots; firmware measurement against references	Test records per device
Commissioning	Removal of default accounts; wireless modules disabled or omitted by a manufacturer-approved method; radio survey; vendor access through the broker only; settings baselines for relays, UPS and ride-through	Hold-point sign-offs by two people; offline signed images
Operation	Monitoring and log retention; patch schedule for edge and BMC; yearly manual-operation and black-start test; three exercises in Section 11; settings change control	Exercise reports; change records; attestation records per server reassignment

Policy recommendations. These are grouped by the body that can act, as in the design paper.

NERC and FERC

1. Add a cyber security requirement to the computational load standards before they are final. It should cover the functions that change load, namely transfer, islanding, reconnection and ramp limits, and the data links the operating-data standard will create. The design paper recommended registering large loads that can island and applying equivalent requirements to their power control systems. NERC’s 2026 registration criteria, revisions to its Rules of Procedure that its Board approved and that NERC filed with FERC on October 21, 2026, do the first by size and connection

voltage rather than by the ability to island; neither they nor the draft standards do the second (NERC Large Loads Action Plan; Power, Oct. 2026).
2. Collect, at registration, the control-system products and remote-service providers each large load depends on. Concentration cannot be managed until it is measured.
3. Require change control and disclosure for the transfer and ride-through settings that governed the July 2026 transfers, coordinated with PJM's proposed ride-through rule.

CISA and the Department of Homeland Security

1. Publish the incident-reporting rule and state plainly whether colocation and build-to-suit operators are covered.
2. Issue a data center profile of the cross-sector performance goals that covers facility controls and management planes, since no federal baseline does.

Congress

1. Enact a multi-year extension of the 2015 information sharing protections before they expire on December 11, 2026. Three short extensions in a year are not a basis for a sharing program.

NIST, the Department of Defense and the intelligence community

1. Publish the high-security AI data center standard called for in July 2025, with a tier commercial operators can build to, and align the defense acquisition framework for AI systems with it.

Utilities and grid operators

1. Add cyber terms to large-load service and interconnection agreements now, without waiting for standards: settings disclosure, notice of change, controls on vendor remote access to load-control equipment, and a voice confirmation procedure.

Processor and memory vendors

1. Deliver memory encryption with integrity and freshness protection. Until then, publish the physical-security assumptions a relying party must verify.

Claims the evidence does not support.

- That hidden disabling devices in Chinese-made inverters have been confirmed. The Department of Energy's review, as reported, found no definitive evidence. The case for removing wireless links does not need that claim.
- That confidential computing lets a tenant treat the facility operator as untrusted. The processor vendors say otherwise.
- That AI has already changed what state actors can do against well-defended networks. Google and Mandiant did not observe that through early 2026. The discovery results justify preparation, not that conclusion.

- That compliance with any current standard amounts to protection against this adversary. No current standard was written for a data center campus that is also a 240 MW grid resource.

15 Limits of the analysis and open items

The conclusions rest on the pattern across many sources and not on any single figure below. The items in this section are disclosed for readers of this working paper. They must be closed before the analysis is used in a filing, a contract, an engineering certification or an investment decision.

Verification status. Sources were opened on October 11, 12, 22 and 23, 2026 with AI research assistance, and the author has read them. Three classes of statement should be distinguished.

- *Opened primary sources.* Government advisories and directives hosted by CISA, NSA, the FBI, NIST, FERC, NERC, the FCC, the White House and CERT Polska; vendor incident reports by Mandiant and Google, Microsoft, Cisco Talos, Dragos, Claroty and Volexity; CVE records and vendor security bulletins; standards-body and project repositories. Figures from these are as reliable as the extraction. Quotations were captured as short extracts through a text-extraction tool and were checked against the source pages by the author.
- *Secondary sources.* Usually marked in the text by phrases such as “as reported” or “law firms report.” The table lists the ones that matter.
- *The author’s estimates and inferences.* Marked as such where they appear: the zone targets, the engineered limits, the log-retention period, the staffing and cost model, the reading of NERC applicability, and the scheduler and vendor-concentration arguments in Section 4.

Item	Current basis	Needed before reliance
ISA/IEC 62443 security-level definitions; use of compensating countermeasures to meet a zone target	Definitions as quoted in vendor copies of 62443-3-3; compensating-countermeasure reading from vendor material, not the 3-2 text	The ISA/IEC 62443-3-2 and 3-3 text
Level 4 certified components	None found for microgrid, relay or battery plant controllers; one firewall operating system reported by a distributor	Certification registries (ISASecure, IECEE)
CISA BOD 26-02, ED 26-01, ED 26-03	Deadlines agree across secondary sources and the joint fact sheet; cisa.gov would not load in this research	The directive texts
NSA control-system zero trust guidance, October 8, 2026	Opened on October 12 and summarized in Section 8	Nothing further
Department of Energy inverter review	Trade press account of an analysis DOE shared with energy-sector partners; no DOE publication found	The DOE analysis

Item	Current basis	Needed before reliance
FCC inverter listing	DA 26-786, DA 26-789, DA 26-870 and the FCC fact sheet opened; the underlying Department of War determinations not opened	Counsel's reading for battery power conversion systems
Defense authorization act sections 842, 847 and 1513	Sections 842, 847 and 1513 read in the official Public Law 119-60 text on October 12	Nothing further; the framework under section 1513 when published
CMMC suspension	Most sources give July 13, 2026; one gives a memorandum dated July 10	The memorandum
NERC computational load drafts	Draft 1 and final-ballot texts of CLO-001-1, CLO-002-1 and CLO-003-1 opened on October 12 and 23; ballot results from NERC's project page; Board adoption and FERC filing pending	The Board-adopted text and the FERC filing
NERC reliability guideline, chapter 7	Chapter text opened on October 12 from the April 2026 preliminary text; the May 2026 issued version was not compared	NERC's issued copy
CIP-003-9 vendor access requirement	Regional entity summaries quoting requirements 6.1–6.3	The standard
UK, EU and Singapore regimes	UK Bill text, EU regulation, Singapore Bill 20/2026 and the ministry's release opened; Singapore commencement status from law firms; the Bill's passage from Parliament's record of bills	Singapore commencement order and the Act as assented to
Department of Defense Level 3 cost estimate	Law-firm and press reproductions; the Federal Register text cut off before the cost analysis	89 FR 83092 regulatory impact analysis
Claroty and Trend Micro exposure measurements	Vendor telemetry and internet scanning; Claroty's tables are not fully consistent with each other	Treat as indicative
Cost model: capital allowance, tools and services allowance, staff counts other than the two operations positions	Author's estimates	Vendor quotations; a staffing review by an operator

Questions this research did not answer.

1. Whether later drafts of the computational load standards will add a security requirement. The first and final-ballot drafts, read on October 12 and 23, contain only CLO-002-1's requirement for a mutually agreeable secure transfer method, and NERC's slides refer security to a working group.
2. What Dominion's root-cause analysis of the July 22, 2026 event says about data center settings. It was due in September 2026 and had not been located on October 22.

3. Whether a standard for the facility itself, beyond NIST's draft SP 800-239 for the computing environment, will be issued under the 2025 plan.
4. When processor vendors will deliver memory encryption with integrity and freshness. Intel says it is evaluating hardening options and developing a way to verify physical ownership, with no date.
5. Data on interference with satellite time and its effect on power system protection. A national laboratory presentation in 2026 notes jamming and spoofing with off-the-shelf equipment but gives no trend data.
6. Whether components certified to ISA/IEC 62443 level 4 exist for microgrid and battery plant controllers.
7. Token-theft volumes for 2026. Microsoft's 2026 report summary gives no volume; one Microsoft campaign report counted more than 35,000 users affected by token theft in a single campaign.

Conflicting figures retained. Google counts 75 zero-days for 2024 in its April 2025 report and 78 in its March 2026 report; this paper cites only the 2025 count. CVE-2024-54085 is scored 9.8 by NIST and 10.0 by AMI. The February 17, 2025 load event is about 1,500 MW in one PJM document and about 1,800 MW in another. Attribution of the Polish attack differs between CERT Polska and Dragos. DARPA corrected its challenge results after first publication; the corrected figures are used. Nozomi scores the Niagara flaws between 4.1 and 7.7, while a press report gives 9.8 for several.

Rules in draft. NERC's computational load standards, which await Board adoption and FERC approval, its disturbance-performance project opened on October 21, 2026, its registration criteria, filed with FERC on October 21, 2026 and awaiting approval, the incident-reporting rule, the supply-chain revisions FERC ordered, the acquisition rules under Executive Order 14412, the defense framework for AI systems, PJM's large-load tariff filing and the UK Bill can each change the legal analysis within months.

Review status. The design paper was reviewed in five external rounds and then audited citation by citation. That process found real errors. This paper has had the following checks. A separate AI reviewer compared every factual statement with the research record and reopened about thirty sources; its corrections were applied. Two external reviewers, each with web access, reviewed Sections 1–14 on October 11, 2026 (Appendix A), the corrected text with every link on October 12 (Appendix B), and the text as corrected again on October 12 (Appendix C). Three research agents reopened primary sources for the open items; three more opened each of the 182 distinct links in Sections 1–15 and compared the page with the statement it supports; a fourth did the same for the 37 links added afterward. The corrections from all of these are applied. On October 22 and 23, 2026 the statements that depend on the date were re-checked against their sources, and the NERC final-ballot texts and ballot results, NERC's new disturbance-performance project, Singapore's parliamentary record, the White House review list and the UK sitting date were opened; Appendix C records those changes. On October 23 both models reviewed the text once more; their findings and dispositions are rows 22 to 25 of Appendix C.

ANNEX

Appendices

Appendix A. Disposition of external review, round 1

On October 11, 2026 Sections 1–14 were given, without hyperlinks, to two external reviewers, each with web search, with instructions to verify 22 groups of claims against primary documents, recompute the arithmetic, list errors and give a verdict. Both found the draft not fit to post without corrections. One reviewer's work was the more thorough. Each finding was checked against a source before it was accepted. Three research agents separately reopened primary sources for the items in Section 15.

#	Reviewer	Finding	Disposition
1	Reviewer A	Claroty’s 18% is one hop from a system making risky outbound connections, not from an internet-exposed system	Accepted after checking Claroty’s own summary. Sections 1 and 3 corrected
2	Reviewer A	No source says the 14-day median is dominated by ransomware	Accepted. The claim was an inference in the research notes. Removed
3	Reviewer A	A mean of minus seven days does not show exploitation is routinely pre-patch	Partly accepted. The words are Mandiant’s; now attributed and qualified
4	Reviewer A	A fault-caused transfer is not proof of what commanded transfers would do	Accepted. Sections 1 and 3 now say the size is shown and the electrical effect has not been modeled
5	Reviewer A	FCC DA 26-870 of August 20, 2026 replaced the inverter definition; wired links now count	Accepted after opening DA 26-870. Section 9 rewritten
6	Reviewer A; agent	AA26-097A July update is primary and co-sealed by seven agencies	Accepted. Section 3 cites the update
7	Reviewer A	SL 4 cannot be claimed through compensating controls; certified components were not found	Accepted. Section 6 now treats level 4 as a target and requires a system assessment
8	Reviewer A	One-way transfer conflicts with polling into protection zones	Accepted. Monitoring zone now receives pushed data only
9	Reviewer A	Islanding permissive must not delay protection; converter limits are programmable	Accepted. Engineered limits 3 and 4 revised
10	Reviewer A	Local-only setting changes may conflict with utility operations	Accepted. Limit 6 allows an authenticated remote connection for utility-required settings
11	Reviewer A	Cooling at level 2 needs a consequence analysis for common-mode loss	Accepted
12	Reviewer A	Removing radio modules can void listings	Accepted. Disablement by manufacturer-supported method
13	Reviewer A	NERC applicability reading too categorical	Accepted. Section 6 qualified

#	Reviewer	Finding	Disposition
14	Reviewer A	CMMC: Phase 2 was suspended, not certification generally	Accepted. Section 12 corrected
15	Reviewer A	Signature checks do not stop SolarWinds-type compromise	Accepted. Section 9 control expanded
16	Reviewer A	BadRAM had a fix; the five attacks differ	Accepted. Section 1 and the Section 7 table corrected against the researchers' pages
17	Reviewer A	BMC log clearing conflicts with evidence retention; GPU power-cycle insufficient	Accepted. Return-to-service steps revised
18	Reviewer A	Post-quantum rollout to all management traffic is not feasible now	Accepted. Staged by device support
19	Reviewer A	ITAR encryption carve-out has further conditions	Accepted. Section 12 qualified
20	Reviewer A	27 people cannot fill 27.4 positions	Accepted. Low case is 28 people, $5.2 million labor, $9.2 million total
21	Reviewer A	Isolation does not remove the need to patch; decoy use can be innocent; RAND level 4 is not a building	Accepted. Sections 5, 10 and 11 revised
22	Reviewer A	Omissions: PJM ride-through proposal; RAND RR-A4704-1; UK large-load controllers	Accepted after opening each. Added to Sections 3, 10 and 12
23	Reviewer A	Section 15 missing; links missing	Rejected. Both were removed from the review copy by design
24	Reviewer A	UK report stage scheduled for October 26	Accepted in round 2. The stages page lists report stage for October 26, 2026; the main Bill page shows no date
25	Reviewer B	BRICKSTORM 393 days should be attributed to Google, not Mandiant	Rejected. The figure appears in the Google and Mandiant investigation report and in Mandiant's M-Trends 2026 executive edition (PDF); the text now attributes it to both
26	Reviewer B	The 91-second figure is not stated by PJM	Accepted. PJM's September account says about 2,900 MW, then about 1,000 MW a minute later; the text uses PJM's words
27	Reviewer B	Regulatory claims rest on secondary sources	Accepted. Primary sources added where they opened; the rest listed in Section 15
28	Agents	BOD 26-02 removal ends at 18 months; CIRCIA confirmed at OIRA; CVE-2026-24260 is July 2026; fabric flaw is CVE-2026-24170 in UFM Enterprise; NIST draft SP 800-239 exists; Singapore provisions not in force	Applied. The CVE-2026-24260 date was later corrected to June 30, 2026 (Appendix B, row 27)

Appendix B. Disposition of external review, round 2, and the citation audit

On October 12, 2026 the corrected text of Sections 1–15 and Appendix A, with every hyperlink, was given to two external reviewers, each with web search, with instructions to confirm each round-1 fix, open every link and judge whether it supports its statement, list remaining errors and give a verdict. Reviewer A reported 14 must-fix and 17 should-fix items and judged the paper fit to post after the must-fix items; Reviewer B reported three must-fix items and the same verdict. Separately, three research agents opened each of the 182 distinct links in Sections 1–15: 172 resolved as written, 10 failed or were malformed, and the page supported the attached statement fully in 136 cases, partly in 35, not at all in 2, and could not be judged in 9. Support was judged on the page as opened, or on an alternate copy or corrected address where the link as written failed; four of the ten failed links were judged that way. Each finding below was checked against a source before it was accepted.

#	Source	Finding	Disposition
1	Reviewer A	PJM's September 15 account revises the July 22, 2026 event to about 3,900 MW in two stages a minute apart, and gives 1,800 MW, 60.042 Hz and 1.05 per unit for February 2025	Accepted after opening the PJM deck. Sections 1, 3 and 4 corrected; the earlier 3,800 MW figure is noted
2	Reviewer A	The BES exclusion also requires the generation to sit behind the retail meter	Accepted after opening the BES definition. Section 6 corrected
3	Reviewer A	The Section 12 table said CIP applies only if registered for onsite generation and assumed low impact	Accepted. Row rewritten
4	Reviewer A	Zero-ingress protection zone conflicts with remote setting changes	Accepted. Remote-changeable settings are now confined to the Utility interface DMZ and Power control zone, never protection relays
5	Reviewer A	Relays are programmable and a trip is a step change, not a rate limiter	Accepted. Engineered limit 4 rewritten with a manufacturer-defined limiter under separate write authority and a study requirement
6	Reviewer A	Section 14 still said wireless modules are removed	Accepted. Section 14 aligned with Section 6
7	Reviewer A	UK large load controllers are aggregators of consumer appliances at 300 MW, not a campus microgrid	Accepted after opening the government factsheet. Section 12 corrected
8	Reviewer A; Reviewer B	Lords report stage is scheduled for October 26, 2026	Accepted after opening the stages page. Section 12 and Appendix A row 24 corrected
9	Reviewer A	The claim that none of the NERC drafts secures the new links cannot be made without reading the drafts	Accepted. Section 12 qualified to NERC's own summary
10	Reviewer A	CMMC: Phase 1 self-assessments continue; cite the Department	Accepted. Row corrected; DoD CIO page cited
11	Reviewer A	"They do not protect against a party with physical access" is too absolute	Accepted. Section 7 limited to the generations and memory types tested
12	Reviewer A	Section 1 turned a mean time to exploit into a general onset time	Accepted. Sections 1 and 5 reworded

#	Source	Finding	Disposition
13	Reviewer A	Chapter 7 of the NERC guideline is readable and names five CIP standards	Accepted after extracting the chapter from the PDF. Section 12 row rewritten; Keentel citation dropped
14	Reviewer A	Secondary sources where primaries exist: CIRCIA proposal, CISA 2015 sunset, CMMC, Virginia code, SEC rule, NIST SP 800-53 catalog, RAND, attack research pages, CMMC costs, BLS wage	Accepted. Primary links added or substituted in Sections 3, 7, 8, 9, 11, 12 and 13
15	Reviewer A	WireTap was disclosed in September 2025; TEE.fail reached GPU attestation by relaying through the processor	Accepted. Section 7 table and note corrected
16	Reviewer A	Decoy credential alarm still too categorical; cooling fallback setpoints may be unsafe; permissive must be wired independently of SCADA; firmware review not universally available; RAND level 5 wording	Accepted. Sections 6, 7, 10 and 11 reworded
17	Reviewer A	CIRCIA coverage test and EU scope stated too simply	Accepted. Section 12 reworded
18	Reviewer A	Cost figures are a declared model, not observed costs; show exact results	Already stated; exact results added to Appendix B below
19	Reviewer A	393 days not shown in M-Trends landing page	Partly accepted. The executive edition PDF states it; Sections 1 and 3 now attribute the figure to Google and Mandiant jointly and Appendix A row 25 cites the PDF
20	Reviewer B	The NSA control-system guidance is public and should be read	Accepted. Opened on October 12 and summarized in Section 8
21	Reviewer B	No PJM source gives 1,800 MW for February 2025	Rejected. PJM’s September 15, 2026 deck gives approximately 1,800 MW
22	Agents	Claroty says one hop, not no more than one; its 0.4% differs from its own counts; the 18% wording	Accepted. Sections 1 and 3 corrected; the discrepancy is stated
23	Agents	Talos dates the campaign, not the exploit, to 2023; GTIG says the tool could capture logins; F5 says accessed, not stole; Volexity describes DNS poisoning, not altered updates	Accepted. Section 3 table reworded
24	Agents	The AI-ramp concern comes from a developer’s slide in the task force materials	Accepted. Section 4 reworded
25	Agents	NSA press release does not state 91 activities; the primer does	Accepted. Primer cited
26	Agents	Intel pages do not say no mitigation for DDRop; Dark Reading and The Hacker News do not support the host-control claim	Accepted. Section 7 table and note corrected
27	Agents	CVE-2026-24260 bulletin dated June 30, 2026	Accepted

#	Source	Finding	Disposition
28	Agents	D3FEND repository README does not define decoys; CISA playbook link failed; AC-3(2) catalog file unreadable; OpenSSH manual page truncated	Accepted. Technique pages, the tool's own page, the NIST PDF and openssh.org/pq.html cited
29	Agents	CRS R48878 does not describe a review of NSM-22 or mention data centers; CISA sector page does not name data centers	Accepted after reading the report and EO 14239. Section 12 row rewritten
30	Agents	22 CFR 120.54 does not name Russia; Latham does not say until further notice; Bisnow says frequently; GAO landing page lacks the update statement; SLSA version not stated on the cited page	Accepted. Each corrected or re-cited
31	Agents	gov.uk, Simpson Thacher and CSA Singapore links malformed in the review copy	The published document's links are intact; the gov.uk trailing period removed
32	Agents	Caliptra registry page does not support the LMS or ML-DSA statement	Accepted. Caliptra README cited for both
33	Agents	Microsoft page does not say servers keep booting	Accepted. Section 7 reworded to Microsoft's statement

Exact results behind the rounded figures in Section 13. 28 × $185,000 = $5,180,000; 29 × $250,000 = $7,250,000; totals $9,180,000 and $14,000,000; 2,015 GWh ÷ 8,760 h = 230 MW average; $9.18–14.0 million ÷ 2,015,000 MWh = $4.56–6.95 per MWh; share of the $46 million resilience premium 20.0–30.4%; share of $5 billion 0.18–0.28%; two weeks of $42 million a month is about $19.3 million at 365 ÷ 12 days per month; $10–25 million ÷ $3.52 billion = 0.28–0.71%; 2 × 8,760 ÷ 2,080 and ÷ 1,780 = 8.42–9.84 positions; total 27.4–28.8 positions.

Appendix C. Disposition of external review, rounds 3 and 4, and the October re-check

On October 12, 2026 the text as corrected after round 2, with every hyperlink, was given to two external reviewers, each with web search, with instructions to confirm every prior fix, verify every claim and citation, recompute the arithmetic and give a verdict. Reviewer A reported five must-fix and ten should-fix items and judged the paper not ready until they were resolved, naming the categorical statement about the NERC drafts as the most serious; Reviewer B reported no must-fix items and judged the paper ready as it stood. A fourth research agent opened each of the 37 links added after the round-2 audit. Each finding was checked against a source before it was accepted. Both models confirmed the arithmetic in Section 13 and the PJM, BES, RAND, BLS and post-quantum figures. Rows 20 and 21 record the re-check of date-dependent statements on October 22 and 23, 2026. On October 23 the text as it then stood, with every link, was given to Reviewer A (High reasoning, about 18 minutes over two replies) and Reviewer B (Expert, under two minutes) for a fourth round. Reviewer A reported five must-fix and nine should-fix items, confirmed the arithmetic and the PJM, NERC ballot, CIRCIA, BLS, RAND, NIST and ITAR figures, and judged the paper ready after the must-fix items, naming the command paths in Section 6 as the most serious; Reviewer B reported no must-fix items, confirmed the arithmetic and judged the paper ready. Rows 22 to 25 record the dispositions.

#	Source	Finding	Disposition
1	Agent	Claroty's 0.4% figure is in the report, not the blog	Accepted. Section 3 cites the report

#	Source	Finding	Disposition
2	Agent	The SEC Item 1.05 row cited the Form 8-K regulation, not the adopting release	Accepted. Release No. 33-11216, 88 FR 51896, cited
3	Agent	The DoD CIO page does not define external service providers; its address failed in one letter case	Accepted. 32 CFR 170.4 added; address corrected
4	Agent	The UK factsheet does not describe the June–September consultation	Accepted. The factsheet now supports the definition; DESNZ supports the consultation
5	Agent	BadRAM's page says less than $10; NIST AC-3(2) says organizations consider the safety risk; SLSA levels are on the build-track page	Accepted. Each reworded or re-cited
6	Agent	The CIRCIA sector criterion could not be confirmed within the tool's reading limit	Confirmed from proposed § 226.2(b)(12)(i), read in the full Federal Register text
7	Reviewer A	Sections 1 and 14 asserted that the NERC drafts contain no cyber requirement while Section 12 said the drafts were not read	Accepted. CLO-001-1, CLO-002-1 and CLO-003-1 were opened; Sections 1, 12 and 15 restated from their text
8	Reviewer A	The ITAR row omitted the sending-from and intended-recipient conditions	Accepted after reading § 120.54(a)(5) and (b). Row rewritten
9	Reviewer A	DA 26-870's domestic-production exclusions were omitted	Accepted after checking the notice. Sentence added to Section 9
10	Reviewer A; Reviewer B	Singapore's status was stale; the Digital Infrastructure Bill was introduced on September 8, 2026	Accepted after opening the ministry's release and the Bill. Section 12 rewritten; the Bill's passage on October 7 was confirmed from Parliament's bills record on October 22
11	Reviewer A	Section 15 made closure of its items a condition of publication	Accepted. Reworded to a condition of reliance
12	Reviewer A	The UK 300 MW figure is not a data centre threshold	Accepted. Sentence corrected
13	Reviewer A	Wireless, battery-limit and VPN wording in Sections 9 and 14 was stricter than Sections 6 and 8	Accepted. Aligned
14	Reviewer A	The remote-intruder sentence in Section 7 and the level 5 sentence in Section 10 were too absolute	Accepted. Reworded; the level 5 sentence now carries RAND's qualifier
15	Reviewer A	Cite the public law rather than the enrolled bill; the OIRA list did not open in its tool; the audit counts need a method note	Accepted. Public Law 119-103 opened and cited; the review page added beside the list; method clause added
16	Reviewer A	Section 847's operative text had not been opened	Accepted. Sections 842, 847 and 1513 read in the official Public Law 119-60 text; Sections 9 and 10 restated
17	Reviewer A	Appendix A row 28 gives the wrong month; the Section 3 table attributes 393 days to Google alone; Section 7 omits the Caliptra README	Accepted. Each corrected

#	Source	Finding	Disposition
18	Reviewer B	Add primary links for Singapore	Accepted (row 10)
19	Reviewer B	The statement that the author had not yet read the sources may be flagged by readers	Resolved in version 1.0: the author has since read the sources
20	Re-check, Oct. 22–23	Date-dependent statements re-checked: the incident-reporting final rule still under White House review; the NERC computational load package passed its final ballot on October 14 and a disturbance-performance project opened on October 21; Singapore's Bill passed on October 7 in Parliament's record; the CMMC task-force report not public; the UK report stage still listed for October 26; SP 800-239 still a draft; no Dominion root-cause analysis, section 1513 framework or AI information sharing center found	Applied. Sections 1, 3, 10, 12 and 15 and the byline updated; the sources opened are listed at the end of the References
21	Re-check, Oct. 23	An interim edit attributed the initial-ballot approval figures to the final ballot, dated the final-ballot posting October 7 and called an ERCOT presentation a NERC update	Corrected from NERC's project page: final ballot October 9–14, weighted segment approval 82.3%, 78.1% and 82.7%; the presentation attributed to ERCOT
22	Reviewer A, round 4	Section 6 said commands reach the control zones only from the control room while also allowing utility signals and remote setting changes; the BES inclusion omitted the 20 MVA unit criterion; the EU regime has no megawatt threshold; the $9–14 million program omits physical guarding and the level 4 enclave; recommendation 1 conflated the draft standards with the registration criteria	Accepted. Section 6 names the two defined exceptions and both inclusion criteria; Section 12 limits the threshold statement to the UK and Singapore; Sections 1 and 13 state the scope of the cost model; recommendation 1 and Section 12 now cite NERC's registration criteria, approved by its Board and filed with FERC on October 21, 2026, from NERC's action-plan page
23	Reviewer A, round 4	Name the three CLO-002-1 requirements that carry the secure-transfer clause; distinguish Covington's September 21 report from the October 23 search; qualify the model-weight sentence, the BLS wage proxy, the ITAR heading and the GPU clearing step; the final-ballot percentages and the Project 2026-03 dates were not readable in its tools	Accepted and reworded in Sections 7, 10, 12 and 13. The ballot results and the Project 2026-03 dates were read directly from NERC's project pages on October 23 and are cited there
24	Reviewer A, round 4	Singapore's passage should rest on a readable parliamentary record	Retained. Parliament's bills record, opened on October 22, lists the Bill as passed on October 7, 2026; a law firm's note of October 15 is cited beside it
25	Reviewer B, round 4	State the day-count basis for two weeks of the monthly carrying cost; confirm the final-ballot percentages against NERC's page	Accepted. Appendix B states the 365 ÷ 12 basis; the percentages were read from NERC's project page on October 23

NOTE AND SOURCES

References

All links were opened on October 11, 12, 22 or 23, 2026 unless Section 15 says otherwise.

Threat assessments and aggregate data

- ODNI, Annual Threat Assessment of the U.S. Intelligence Community, March 2026
- Mandiant, M-Trends 2026, March 23, 2026
- Verizon, 2026 Data Breach Investigations Report
- Google Threat Intelligence Group, 2025 zero-day review, March 5, 2026
- CISA, Known Exploited Vulnerabilities catalog data, version of October 8, 2026 (1,739 entries)

State campaigns against IT infrastructure

- CISA, NSA, FBI and partners, AA24-038A, PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure, February 7, 2024
- NSA, CISA, FBI and partner agencies of twelve other countries, Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide, August 27, 2025
- Cisco Talos, Salt Typhoon analysis, February 20, 2025; UAT-8616 and Cisco SD-WAN, February 25, 2026
- CISA, Emergency Directive 25-03, September 25, 2025
- Netherlands NCSC, MIVD and AIVD, COATHANGER advisory and follow-up, 2024
- Mandiant, Juniper routers and UNC3886, March 12, 2025; vCenter exploitation since 2021, January 19, 2024
- Google Threat Intelligence Group, BRICKSTORM espionage campaign, September 24, 2025; UNC6201 and Dell RecoverPoint, February 17, 2026
- CISA, NSA and Canadian Centre for Cyber Security, AR25-338A, BRICKSTORM Backdoor, December 4, 2025, updated December 19, 2025
- Cyber Safety Review Board, Review of the Summer 2023 Microsoft Exchange Online Intrusion, March 20, 2024
- Microsoft, Midnight Blizzard guidance, January 25, 2024; Silk Typhoon, March 5, 2025
- GAO, GAO-22-104746, Federal Response to SolarWinds and Microsoft Exchange Incidents, January 2022
- F5, Lessons from our security incident, October 22, 2025
- Volexity, StormBamboo compromises an ISP, August 2, 2024
- NIST National Vulnerability Database, CVE-2024-54085; CVE-2024-3094
- Eclypsium, BMC vulnerability added to the exploited list, June 26, 2025
- Nextgov, report on Salt Typhoon and data center providers, June 9, 2025

Control systems, facility systems and grid events

- SANS and E-ISAC, Analysis of the Cyber Attack on the Ukrainian Power Grid, March 18, 2016
- U.S. Department of Justice, charges against six GRU officers, October 19, 2020
- CISA, FBI and DOE, AA22-083A, March 24, 2022
- Mandiant, Sandworm disrupts power in Ukraine, November 9, 2023
- Dragos, FrostyGoop intelligence brief, July 2024; Poland attack, January 28, 2026; 2026 Year in Review release, February 17, 2026
- CERT Polska, Energy Sector Incident Report 2025; Follow-up Report, 2026
- FBI, CISA, NSA, EPA, DOE and U.S. Cyber Command, AA26-097A, Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers, April 7, 2026; Industrial Cyber on the July 2026 update
- Trellix, The Threat Lurking in Data Centers, August 12, 2023
- Claroty Team82, UPS network cards and press release, June 9, 2026; State of CPS Security: Data Center Exposures, July 29, 2026
- CISA, ICSA-25-140-10; ICSA-25-203-06
- Nozomi Networks, Tridium Niagara vulnerabilities, July 23, 2025
- TrendAI Research, Industrial control systems exposed near data centers, August 8, 2026
- NERC, Incident Review: Considering Simultaneous Voltage-Sensitive Load Reductions, January 8, 2025; CIP Roadmap, January 2026; Large Loads Task Force presentations, August 28, 2025; Level 3 alert, May 4, 2026
- PJM, Operating Committee presentation on the July 22, 2026 event, August 6, 2026; Inside Lines, August 11, 2026; Planning Committee presentation, September 15, 2026
- FCC, Public Notice DA 26-786, July 28, 2026; Squire Patton Boggs and K&L Gates summaries
- pv magazine USA, DOE inverter review, January 28, 2026; CIP-003-9 vendor access, April 22, 2026

Automation and vulnerability discovery

- Anthropic, Disrupting the first reported AI-orchestrated cyber espionage campaign, November 2025; Cyber Verification Program, October 6, 2026
- DARPA, AI Cyber Challenge results, August 8, 2025
- UK AI Security Institute, evaluation of Claude Mythos Preview's cyber capabilities, April 13, 2026
- Google Threat Intelligence Group, AI Threat Tracker, February 12, 2026

Platform, firmware and confidential computing

- NIST, SP 800-193, Platform Firmware Resiliency Guidelines, May 2018; SP 800-88 Rev. 2, September 26, 2025
- NSA, BMC hardening release, June 14, 2023; Hardware and Firmware Security Guidance
- CHIPS Alliance, Caliptra approved products registry; Caliptra 2.0 specification
- Open Compute Project, S.A.F.E. reports
- CVE records: CVE-2026-11835; CVE-2026-16141; CVE-2026-79820; CVE-2026-21265; CVE-2024-21944
- Microsoft, Secure Boot certificate updates for servers, February 23, 2026; Red Hat, article 7128933, September 22, 2026
- AMD, AMD-SB-3024; AMD-SB-3040; AMD-SB-3048
- Intel, announcement of October 28, 2025; announcement on DDRop, September 14, 2026
- SecurityWeek, WireTap, October 2, 2025; Dark Reading, Battering RAM, October 1, 2025
- Cloud Security Alliance, research note on DDRop, September 16, 2026
- NVIDIA, bulletin 5850, June 30, 2026; bulletin 5809, August 25, 2026; protected multi-GPU mode
- RAND, Securing AI Model Weights, RR-A2849-1, May 30, 2024

Network, identity and cryptography

- CISA, Binding Operational Directive 23-02; edge device guidance, February 4, 2025
- Cisco, summary of Binding Operational Directive 26-02, May 4, 2026; BleepingComputer, report of February 6, 2026
- CISA, FBI and partners, Modern Approaches to Network Access Security, June 18, 2024
- NIST, SP 800-207, August 2020; SP 800-63B-4, 2025; SP 800-53 Rev. 5, release 5.2.0
- NSA, Zero Trust Implementation Guideline Primer, January 2026; release of January 30, 2026; control-system zero trust release, October 8, 2026
- NSA, CSfC Key Management Requirements Annex v3.0.0 and Symmetric Key Management Annex 3.0.0, March 27, 2026
- Cloudflare, DDoS report, Q4 2025; H1 2026
- Office of the National Cyber Director, Roadmap to Enhancing Internet Routing Security, September 2024
- NIST, FIPS 203, August 13, 2024; IR 8547 initial public draft, November 12, 2024; IR 8323 Rev. 1, January 2023

- NSA, CNSA 2.0 FAQ, version 2.0, April 2024; post-quantum announcement, October 1, 2026; position on quantum key distribution
- Executive Order 14412, Securing the Nation Against Advanced Cryptographic Attacks, June 22, 2026
- OpenSSL, release notes; OpenSSH, client configuration manual

Supply chain, detection and response

- SLSA, build levels, specification v1.2
- Eclipse Foundation, Cyber Resilience Act timeline
- FERC, Order No. 912, September 18, 2025
- Baker McKenzie, summary of the FY2026 defense authorization act
- MITRE, D3FEND ontology
- CISA, Eviction Strategies Tool
- Idaho National Laboratory, Cyber-Informed Engineering
- Lloyd's, Market Bulletin Y5381, August 17, 2022
- Congressional Research Service, IF12959, September 3, 2026; R48878, March 10, 2026
- Security.io, CIRCIA final rule enters review, October 5, 2026; REN-ISAC, reproduction of the proposed rule

Law, regulation and policy

- White House, President Trump's Cyber Strategy for America, March 2026; America's AI Action Plan, July 2025
- CISA, Information Technology Sector
- FERC, order in Docket RD26-7-000, July 16, 2026; Willkie, summary
- NERC, BES definition; CIP-002-5.1 application guide; bulletin of August 24, 2026; Reliability Guideline: Risk Mitigation for Emerging Large Loads; Texas RE, computational load proposal presentation; Keentel, guideline summary
- Latham & Watkins, CMMC Phase 2 suspension, July 30, 2026; 32 CFR 170.19
- NIST, SP 800-172 Rev. 3 announcement, May 13, 2026; SP 800-82 Rev. 3, September 2023
- DISA, Cloud Service Provider Security Requirements Guide, V1R2, January 30, 2025
- 22 CFR 120.54
- GAO, B-337935, May 12, 2026; BIS, Data Center Validated End User rule, 89 FR 80080
- Crowell & Moring, FY2026 defense authorization act, Section 1513, January 7, 2026

- SEC comment file, CTIA letter, October 2, 2026; TSA, security directives; Virginia Attorney General, breach notification summary
- UK government, data centres designated critical national infrastructure, September 12, 2024; UK Parliament, Cyber Security and Resilience Bill; HSF Kramer, summary
- Hunton, EU implementing regulation 2024/2690; Cyber Security Agency of Singapore, Cybersecurity (Amendment) Bill; Ministry of Digital Development and Information, New Digital Infrastructure Bill, September 8, 2026; Parliament of Singapore, Digital Infrastructure Bill, Bill No. 20/2026; W.Media, Singapore's Digital Infrastructure Bill passed in Parliament, October 8, 2026
- ASD and partners, Principles of Operational Technology Cyber Security; Utility Dive, CISA performance goals 2.0

Cost and staffing

- IANS Research and Artico Search, 2025 Security Budget Benchmark summary; 2026 edition page
- Uptime Institute, Annual Outage Analysis 2026 announcement, May 13, 2026
- Bureau of Labor Statistics, employer costs for employee compensation, June 2026; WageDex, reproduction of May 2025 wage data
- Petronella, reproduction of Department of Defense CMMC cost estimates; SecurityWeek, control-system security budget survey; Bisnow, secure facility construction cost

Additional sources cited in the text

- Congressional Research Service, IN12667, March 11, 2026, for the placement of data centers within the Information Technology Sector
- HSToday, report on Binding Operational Directive 26-02, for CISA's encouragement to non-federal organizations
- Eclypsium, AMI MegaRAC vulnerabilities, March 18, 2025, for the consequences of BMC compromise
- NSA, HIRS project
- XZ Utils project, release notes, for the two affected releases
- BleepingComputer, TEE.fail, October 28, 2025; The Hacker News, DDRop, September 14, 2026
- Reuters, as syndicated by the Hawaii Tribune-Herald, May 15, 2025
- IntelliSee, status of the Section 1513 framework, June 11, 2026
- Davis Wright Tremaine, lapse of the Cybersecurity Information Sharing Act, October 2, 2025; Hunton, extension through September 2026, February 12, 2026
- Simpson Thacher, Merck v. ACE, May 31, 2023; Chambers, Insurance Litigation 2026, New Jersey
- Advisera, NIS2 implementing regulation 2024/2690, January 31, 2025

Sources added after the first external review round (October 11, 2026)

- CISA, FBI and partners, joint fact sheet on BOD 26-02, Feb. 5, 2026.
- FBI, CISA and partners, AA26-097A update, July 22, 2026.
- FCC, DA 26-870, Aug. 20, 2026; DA 26-789, July 28, 2026; fact sheet.
- PJM Planning Committee, large load ride-through presentation, Sept. 8, 2026.
- NERC, computational load update slides, Aug. 2026; American Public Power Association, ballot report.
- OIRA, regulatory actions under review, read Oct. 11 and 12, 2026; Executive Order submissions under review.
- RAND, Achieving AI Model Weight Security Level 3, RR-A4704-1, Aug. 25, 2026.
- NIST, SP 800-239 initial public draft, July 2026.
- UK Parliament, Cyber Security and Resilience Bill, HL Bill 49; DESNZ, Large Load Controllers consultation, June–Sept. 2026.
- Claroty, Data center exposures and the pathways putting data center assets at risk, 2026.
- Cisco Talos, UAT-8616 and Cisco SD-WAN, Feb. 2026.

Sources added after the second review round and the citation audit (October 12, 2026)

- NSA, Hardening Department of War (DoW) Critical Operational Technology (OT) Environments with Zero Trust (ZT) Principles, October 2026; Zero Trust Implementation Guideline primer, January 2026.
- PJM Planning Committee, large computational load ride-through background, September 15, 2026.
- NERC, Reliability Guideline: Risk Mitigation for Emerging Large Loads, April 2026 text, chapter 7.
- UK Parliament, Cyber Security and Resilience Bill stages; UK government, large load controllers factsheet.
- Executive Order 14239, Achieving Efficiency Through State and Local Preparedness, March 18, 2025.
- CISA, Cyber Incident Reporting for Critical Infrastructure Act proposed rule, 89 FR 23644, April 4, 2024; Department of Defense, CMMC program final rule, 89 FR 83092, October 15, 2024; 32 CFR 170.4; DoD CIO, About CMMC.
- Congress, Continuing Appropriations and Extensions Act, 2027, Pub. L. 119-103, Division B § 2011, approved September 2, 2026 (enrolled as H.R. 6500).
- SEC, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11216, 88 FR 51896, August 4, 2023; 17 CFR 249.308; Va. Code § 18.2-186.6; Regulation (EU) 2024/2690.
- Researchers' project pages: BadRAM; WireTap; Battering RAM; TEE.fail; DDRop.

- NIST, SP 800-53 Rev. 5; MITRE D3FEND, decoy user credential and decoy session token; CISA, Eviction Strategies Tool; OpenSSH, post-quantum cryptography; SLSA v1.2; CHIPS Alliance, Caliptra README.
- Bureau of Labor Statistics, Information Security Analysts, Occupational Outlook Handbook; GAO, GAO-22-104746 report; Mandiant, M-Trends 2026 Executive Edition; ReliabilityFirst, CIP-003-9; MRO, CIP-003-9 vendor electronic remote access.
- NERC, Project 2026-02 draft standards, formal posting 1: CLO-001-1, CLO-002-1 and CLO-003-1, August 2026, read October 12, 2026.
- Congress, National Defense Authorization Act for Fiscal Year 2026, Pub. L. 119-60, §§ 842, 847 and 1513, read October 12, 2026.
- Ministry of Digital Development and Information (Singapore), New Digital Infrastructure Bill, September 8, 2026; Parliament of Singapore, Digital Infrastructure Bill, Bill No. 20/2026; W.Media, Singapore's Digital Infrastructure Bill passed in Parliament, October 8, 2026.
- Claroty, Team82 data center report, July 2026; eCFR, 22 CFR 120.54; 32 CFR 170.4; SLSA, build track basics, v1.2.

Sources added after the re-check of October 22–23, 2026

- NERC, Project 2026-02 Computational Loads, final ballot results and postings, read October 23, 2026; final ballot announcement, October 9, 2026; final-ballot texts of CLO-001-1, CLO-002-1 and CLO-003-1, October 2026.
- NERC, Project 2026-03 Computational Loads Disturbance Performance, standard authorization request accepted October 21, 2026; ERCOT, NERC Computational Load Update, October 15, 2026; American Public Power Association, NERC's computational loads standards advance, October 15, 2026.
- Parliament of Singapore, Bills introduced, read October 22, 2026; UK Parliament, Cyber Security and Resilience Bill, Lords report stage, read October 23, 2026.
- NERC, Large Loads Action Plan, read October 23, 2026; Drew & Napier, Upcoming Digital Infrastructure Act, October 15, 2026; Covington & Burling, CMMC reform task force updates, September 21, 2026; Cybersecurity Dive, AI-ISAC update, February 3, 2026; Office of Information and Regulatory Affairs, regulatory actions under review, read October 22, 2026; NIST, SP 800-239 initial public draft page, read October 22, 2026.

SUGGESTED CITATION

George, Collin B. *Data Center Cybersecurity Against Nation-State Operations: Architecture, Technology, Assurance and Cost for 100–300 MW Campuses.* Sanctir Working Paper, WP-2026 series, version 1.0, 23 October 2026. Licensed CC BY-NC-ND 4.0.

AUTHOR

About the author

Collin B. George, CISSP, is National Security Advisor at Sanctir, an independent research and advisory practice working on sanctions, export controls, maritime enforcement and defense industrial base risk.

This paper uses no classified, controlled, or proprietary information and reflects no agency position. The full declaration is in the paper record above.

National Security Advisor, Sanctir LLC, Redmond, Washington · cgeorge@sanctir.com · sanctir.com · ORCID 0009-0007-8162-6839