Cybersecurity for National Security: Roadmaps, Policy, Partnerships, and Acquisitions (DRAFT)

Paul F. Roysdon, Ph.D.

February 14, 2025

Abstract

Cyber risk has become a persistent strategic threat with material impacts to national security, public safety, and economic stability. The United States is shifting from voluntary, outcome-light models to outcome-based regulation, software liability pressure, and memory-safe, post-quantum, zero trust architectures. This paper proposes a 2025–2035 roadmap that integrates policy, engineering, and acquisitions: (i) national milestones for zero trust, post-quantum cryptography, memory-safe software, and incident reporting harmonization; (ii) an Intelligence Community (IC) plan for data fabrics, continuous monitoring, and hunt-forward operations; (iii) governance using the NIST Cybersecurity Framework 2.0; (iv) partnerships via CISA's JCDC and sector risk management agencies; and (v) rapid, modular contracting patterns that tie incentives to measurable security outcomes.

1 Strategic Imperative and Current Posture

Cyber operations by state and criminal actors routinely disrupt hospitals, pipelines, and municipal services, while supply-chain compromises and cloud identity abuse challenge legacy perimeters. Federal direction now orients around: (1) *Zero Trust* adoption across agencies; (2) *software supply chain security* using SSDF and SBOM practices; (3) *operational collaboration* through the Joint Cyber Defense Collaborative (JCDC); (4) *timely incident disclosures* (e.g., SEC Form 8-K Item 1.05) and sectoral reporting; and (5) *post-quantum cryptography* and *memory safety* to reduce classes of defects.

2 Threat Landscape

- **Ransomware and data extortion:** Criminal ecosystems exploit weak identity hygiene, flat networks, and unpatched edge services; double-extortion tactics increase business impact.
- **State-aligned APT activity:** Long-dwell intrusions targeting defense industrial base (DIB), critical infrastructure, and cloud identity providers.
- **Operational Technology (OT) risk:** Pipelines, rail, and water utilities require outcome-based controls and timely incident reporting; segmentation and continuous monitoring remain uneven.
- **Software supply chain:** Vulnerable dependencies and build systems demand SSDF practices, reproducible builds, and verifiable attestations.

- **Regulatory fragmentation:** Multiple overlapping rules drive compliance cost; harmonization and reciprocity are essential to reduce burden while improving outcomes.

3 State of Practice and Standards

3.1 Zero trust

NIST SP 800-207 defines the conceptual architecture; OMB M-22-09 and DoD's Zero Trust Strategy establish federal implementation objectives. [1, 2, 3] Priorities include identity-centric access, continuous authorization, strong device posture, encrypted traffic, and centralized policy decision points.

3.2 Software supply chain security

NIST SP800-218 (SSDF) codifies secure development practices. Executive Order14028 accelerated SBOM, provenance, and high-assurance build requirements, while FedRAMP Rev.5 baselines align cloud security with NIST SP800-53 Rev. 5. [4, 5, 6, 7]

3.3 Memory safety

CISA and partners urge vendors to publish *memory-safe roadmaps* and increase the share of code in memory-safe languages, complemented by mitigations (control-flow integrity, hardened allocators) where rewriting is infeasible.[8]

3.4 Post-quantum cryptography

NIST finalized FIPS203 (ML-KEM), FIPS204 (ML-DSA), and FIPS 205 (SLH-DSA) with effective date August 14, 2024; agencies and critical infrastructure should plan phased migration with crypto-agility and risk scoring for long-lived data. [9, 10, 11]

3.5 Incident reporting and disclosures

The National Cybersecurity Strategy (NCS) and its 2024 Implementation Plan advance harmonized reporting. CIRCIA's rulemaking proposes 72-hour incident and 24-hour ransom-report timelines for covered critical infrastructure, while SEC rules require public companies to report material cyber incidents within four business days. [12, 13, 14, 15]

4 National Cyber Roadmap (2025–2035)

4.1 Phase I—*Harden and Harmonize* (2025–2026)

- **Zero Trust baselines:** Achieve agency ZT target states for identity, device, network, application, and data; adopt continuous authorization and phishing-resistant MFA. [1, 2, 3]
- **PQC pilots:** Deploy ML-KEM/ML-DSA gateways; complete crypto inventories; protect high-value data against harvest-now/decrypt-later. [9, 10, 11]
- **SSDF + SBOM:** Require SSDF-aligned attestations for major acquisitions; mandate SBOMs and vulnerability/exploitability (VEX) metadata. [4, 5]
- **Memory safety:** Each major vendor publishes a roadmap with measurable language migration targets and mitigations. [8]
- **Reporting harmonization:** Align sectoral rules to CIRCIA data elements; enable machine-readable submissions and reciprocity across regulators. [16, 13]

4.2 Phase II—*Operate and Automate* (2027–2029)

- **Continuous monitoring fabric:** Unified telemetry (cloud, endpoint, network, identity) with automated containment, canarying, and kill-switches. [17]
- **Threat-informed defense:** ATT&CK-driven detections; purple-teaming at scale; large-model assistants for triage and hunt.
- **Cross-sector exercises:** JCDC-led exercises with shared playbooks; sector cyber ranges for OT with vendor-in-the-loop testing. [18, 19]
- **PQC at scale:** Transition major protocols (TLS, QUIC, IPsec, PQC-enabled PKI); dual-stack deployments with agility. [9, 10, 11]

4.3 Phase III—*Resilience and Recovery* (2030–2035)

- **Self-healing architectures:** Partitioned blast radii, automated re-provisioning, signed golden images, and continuous dependency risk scoring.
- **Regulatory convergence:** Mature reciprocity across SEC, CIRCIA, TSA, HHS, and sector regulators; outcome metrics emphasize dwell time, lateral-movement prevention, and recovery SLAs. [14, 16, 20, 21]
- **PQC completion:** Full migration for federal high-value assets and critical infrastructure PKI; legacy risk isolated behind PQC gateways. [9, 10, 11]

Table 1: Milestones and Metrics

Year	Domain	Target	Example Metric
2026	ZT	Phishing-resistant MFA	$> 98\%$ protected logins
2026	PQC	Crypto inventory complete	$> 95\%$ coverage
2026	SSDF	SBOM/VEX in new awards	$> 90\%$ by value
2027	Reporting	Machine-readable CIRCIA	$> 90\%$ of covered entities
2028	Telemetry	Unified telemetry fabric	Mean time to contain < 1 h
2029	PQC	PQC-enabled TLS/PKI	$> 80\%$ external services
2031	Resilience	Blast-radius partitioning	$> 95\%$ critical apps segmented
2033	PQC	Full migration HVAs	$> 99\%$ HVA coverage

5 IC Roadmap

5.1 Mission use cases

Counterintelligence and DIB protection; threat emulation and hunt-forward; crypto-agile enclaves; supply-chain verification (SBOM attestation, reproducible builds); PQC transition for classified and controlled networks. [12]

5.2 Infrastructure

Tier-1 Cyber Fusion Campus: petabyte/day telemetry ingest; AI-assisted SOC; red/blue/purple ranges; malware foundry; classified enclaves with cross-domain solutions.

Tier-2 Regional Pods: deployable hunt teams; OT testbeds; data-lake shards with local analytics.

Tier-3 Kits: forward sensors, deception, and PQC gateways.

6 Policy and Governance

- **Framework alignment:** Adopt NIST CSF2.0 with the new *Govern* function as the organizing backbone for agencies and critical infrastructure. [22, 23]
- **Zero Trust mandates:** Maintain OMB M-22-09 targets; extend to grants and regulated sectors via outcome metrics. [2]
- **Software liability and incentives:** Tie procurement preferences and safe harbors to SSDF conformance, memory-safe roadmaps, and vulnerability response SLAs. [4, 8]
- **Reporting harmonization:** ONCD leads interagency harmonization; publish a common data schema and reciprocity matrix. [12]
- **PQC policy:** Set dated milestones aligned to FIPS203/204/205; require crypto-agility in all new systems. [9, 10, 11]

7 Partnerships

7.1 Operational collaboration

Deepen JCDC constructs with cloud/telecom/CDN/identity providers; expand international collaboration (Five Eyes, EU) and cross-sector exercises. [18, 19] Sector risk management agencies align outcome metrics and reciprocity. Additionally, TSA directives for pipeline and rail operators exemplify outcome-based OT cybersecurity requirements. [20, 21, 24, 25]

7.2 Vendors and integrators

Prime integrators for federal and critical-infrastructure deployments; cloud service providers aligned to FedRAMP Rev. 5; security vendors committed to memory-safe roadmaps and verifiable SBOMs.

8 Acquisitions: Rapid, Modular, Accountable

8.1 Outcome-based contracts

Tie incentives to measurable outcomes: phishing-resistant MFA adoption, privileged access reductions, lateral movement prevention, mean time to contain, and recovery SLAs. Require SSDF attestations, SBOM/VEX, and PQC agility. [4, 14]

8.2 Modular CLINs

Separate identity, telemetry, analytics, response orchestration, PQC gateways, and OT security segments to enable independent competition and upgrades. Use OTA and down-select phases for rapid fielding.

9 Facility Blueprint

Security operations leverage a unified data fabric (cloud-native lakehouse), AI-assisted triage, deception, and kill-switch automation. OT cyber ranges validate playbooks against vendor equipment. Classified enclaves maintain cross-domain guards and PQC front-doors. [6]

10 Risk Register

- **Identity compromise:** Enforce phishing-resistant MFA, privileged access management, and continuous authorization.
- **Supply-chain opacity:** Mandate SBOM/VEX, attestations, and reproducible builds; red-team vendor updates.

- **Telemetry gaps:** Require unified collection across cloud, endpoint, network, and identity with strict retention.
- **Regulatory uncertainty:** Plan for litigation risk; prioritize harmonization and standards-based reciprocity.
- **PQC lag:** Fund migration tooling, gateways, and crypto-inventory automation; protect long-lived data now.

11 Conclusion

A defensible national posture requires outcome-driven zero trust, secure-by-design software, rapid incident visibility, and crypto-agility. By aligning policy, partnerships, and rapid acquisitions with measurable engineering milestones, the United States can reduce systemic risk, speed recovery, and sustain technological advantage.

Acknowledgments

The author thanks colleagues across government, industry, and academia for discussions that informed this work.

References

[1] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," NIST, Tech. Rep. Special Publication 800-207, 2020, accessed: July 25, 2025. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

[2] Office of Management and Budget, "Moving the u.s. government toward zero trust cybersecurity principles," OMB Memorandum M-22-09, 01 2022, accessed: July 25, 2025. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[3] Department of Defense Chief Information Officer, "Department of defense zero trust strategy," DoD CIO, Tech. Rep., 2022, accessed: July 25, 2025. [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

[4] M. Souppaya, K. Scarfone, and D. Dodson, "Secure software development framework (ssdf) version 1.1," NIST, Tech. Rep. Special Publication 800-218, 2022, accessed: July 25, 2025. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/218/final

[5] The White House, "Executive order 14028: Improving the nation's cybersecurity," Presidential Executive Order, 05 2021, accessed: July 25, 2025. [Online]. Available: https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[6] FedRAMP Program Management Office, "Rev. 5 baselines have been approved and released!" FedRAMP Blog, 05 2023, accessed: July 25, 2025. [Online]. Available: https://www.fedramp.gov/blog/2023-05-30-rev-5-baselines-have-been-approved-and-released/

[7] ——, "Fedramp baselines rev 5 transition guide," FedRAMP, Tech. Rep., 2023, accessed: July 25, 2025. [Online]. Available: https://www.fedramp.gov/assets/resources/documents/FedRAMP_Baselines_Rev5_Transition_Guide.pdf

[8] CISA, NSA, FBI, ACSC, CCCS, NCSC-UK, NCSC-NZ, CERT-NZ, "The case for memory safe roadmaps," Cybersecurity and Infrastructure Security Agency, Tech. Rep., 12 2023, accessed: July 25, 2025. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-12/The-Case-for-Memory-Safe-Roadmaps-508c.pdf

[9] National Institute of Standards and Technology, "Module-lattice-based key-encapsulation mechanism (ml-kem)," NIST, Tech. Rep. FIPS 203, 2024, accessed: July 25, 2025. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.203.pdf

[10] ——, "Module-lattice-based digital signature standard (ml-dsa)," NIST, Tech. Rep. FIPS 204, 2024, accessed: July 25, 2025. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.204.pdf

[11] ——, "Stateless hash-based digital signature standard (slh-dsa)," NIST, Tech. Rep. FIPS 205, 2024, accessed: July 25, 2025. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.205.pdf

[12] The White House, "National cybersecurity strategy," Office of the National Cyber Director, Tech. Rep., 03 2023, accessed: July 25, 2025. [Online]. Available: https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[13] Cybersecurity and Infrastructure Security Agency, "Circia notice of proposed rulemaking: Informational overview," Briefing document, 04 2024, proposed 72-hour incident and 24-hour ransom reporting timelines. Accessed: July 25, 2025. [Online]. Available: https://www.cisa.gov/sites/default/files/2024-04/CIRCIA%20NPRM%20Overview%20V2%28FINAL%29_508c%20%28locked%29.pdf

[14] U.S. Securities and Exchange Commission, "Cybersecurity risk management, strategy, governance, and incident disclosure," Final Rule, Release No. 33-11216, 07 2023, item 1.05 of Form 8-K requires disclosure within four business days after determining materiality. Accessed: July 25, 2025. [Online]. Available: https://www.sec.gov/files/rules/final/2023/33-11216.pdf

[15] ——, "Cybersecurity risk management, strategy, governance, and incident disclosure," Rulemaking Docket S7-09-22, 2023, effective September 5, 2023; compliance dates vary. Accessed: July 25, 2025. [Online]. Available: https://www.sec.gov/rules-regulations/2023/07/s7-09-22

[16] Cybersecurity and Infrastructure Security Agency, "Cyber incident reporting for critical infrastructure act of 2022 (circia)," Program overview, 2022, requires reporting of covered cyber incidents within 72 hours and ransom payments within 24 hours. Accessed: July 25, 2025. [Online]. Available: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

[17] Office of Management and Budget, "Fiscal year 2025 guidance on federal information security

and privacy management requirements," OMB Memorandum M-25-04, 01 2025, aligns FISMA metrics with Zero Trust and NCS implementation. Accessed: July 25, 2025. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2025/01/M-25-04-Fiscal-Year-2025-Guidance-on-Federal-Information-Security-and-Privacy-Management-Requirements.pdf

[18] Cybersecurity and Infrastructure Security Agency, "Joint cyber defense collaborative (jcdc)," Program page, 2021, accessed: July 25, 2025. [Online]. Available: https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative

[19] ——, "Jcdc faqs," FAQ, 2021, accessed: July 25, 2025. [Online]. Available: https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative/jcdc-faqs

[20] Transportation Security Administration, "Security directive pipeline-2021-02f: Pipeline cybersecurity mitigation actions, contingency planning, and testing," Security Directive, 05 2025, effective May 3, 2025; expires May 2, 2026. Accessed: July 25, 2025. [Online]. Available: https://www.tsa.gov/sites/default/files/tsa-security-directive-pipeline-2021-02f-and-memo-508c.pdf

[21] ——, "Security directive 1580/82-2022-01c: Rail cybersecurity mitigation actions and testing," Security Directive and Correction Memo, 07 2024, effective July 1, 2024; expires May 2, 2025. Accessed: July 25, 2025. [Online]. Available: https://www.tsa.gov/sites/default/files/tsa-security-directive-1580_82-2022-01c-and-memo-508c.pdf

[22] National Institute of Standards and Technology, "The nist cybersecurity framework (csf) 2.0," NIST, Tech. Rep. NIST CSWP 29, 02 2024, accessed: July 25, 2025. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[23] ——, "Nist releases version 2.0 of landmark cybersecurity framework," 02 2024, announces the new
emphGovern function. Accessed: July 25, 2025. [Online]. Available: https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework

[24] Transportation Security Administration, "Security directive pipeline-2021-01b: Enhancing pipeline cybersecurity," Security Directive, 05 2022, requires incident reporting to CISA within 24 hours and designating a Cybersecurity Coordinator. Accessed: July 25, 2025. [Online]. Available: https://www.tsa.gov/sites/default/files/sd_pipeline-2021-01b_05-29-2022.pdf

[25] ——, "Tsa issues new cybersecurity requirements for passenger and freight railroad carriers," Press Release, 10 2022, accessed: July 25, 2025. [Online]. Available: https://www.tsa.gov/news/press/releases/2022/10/18/tsa-issues-new-cybersecurity-requirements-for-passenger-and-freight