Cybersecurity Under the Second Trump Administration: What to Watch for in 2025

April 9, 2025

Caitlin M. Clarke
Senior Director of Cybersecurity Services | +1 202.344.4493 | cmclarke@Venable.com

Ross B. Nodurft
Senior Director of Cybersecurity Services | +1 202.344.4403 | rbnodurft@Venable.com

Alexander Botting
Senior Director, Global Security and Technology Strategy | +1 202.344.4440 | abotting@Venable.com

VENABLE LLP

Navigating Policy Shifts Under a Second Trump Administration

As we look ahead to a new political landscape, join us for a series of webinars that will offer insights into the key regulatory and policy changes expected under a second Trump presidency.

We'll explore how leadership transitions, executive actions, and congressional dynamics will shape the future of industries that include, among others, healthcare, financial services, energy, and trade.

Each session will feature analysis from Venable attorneys and senior policy advisors, providing actionable guidance on how businesses and organizations can navigate the evolving policy landscape. Join us for a comprehensive look at the changes coming to Washington in 2025 and beyond.

Key Players

Sean Cairncross: Nominated as the national cyber director. Previously served as the CEO of the Millenium Challenge Corporation under the first Trump administration and held a leadership role within the Republican National Committee.

Alexei Bulazel: Serving as the special assistant to the president and senior director for cyber on the National Security Council (NSC). Previously served on the NSC in 2020-2021 and held several positions within technology companies.

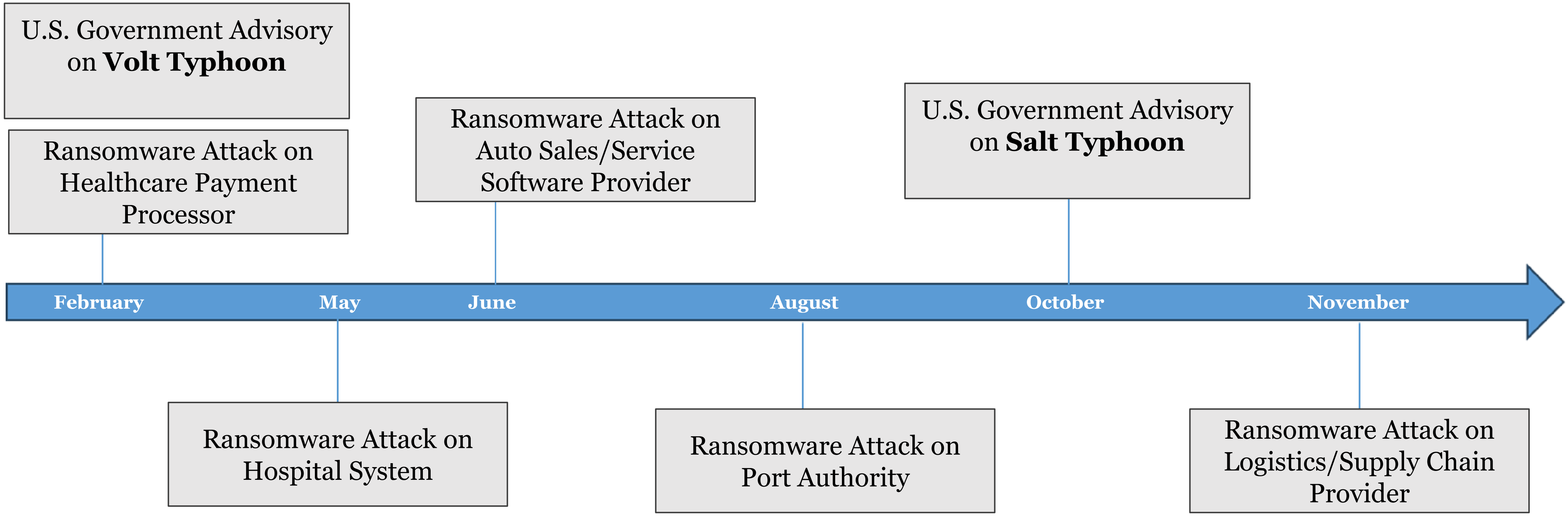
Sean Plankey: Nominated as the director of the Cybersecurity and Infrastructure Security Agency (CISA). Previously served on the NSC from 2018 to 2019 and as principal deputy assistant secretary for cybersecurity, energy security, and emergency response at the Department of Energy during the first Trump administration.

Katie Sutton: Nominated to serve as the assistant secretary of defense for cyber policy. Currently the chief technology advisor to the commander and director of Pentagon Operations at U.S. Cyber Command.

Katie Arrington: Currently performing the duties of the chief information officer; appointed as the chief information security officer. Previously served as the CISO for the acquisition and sustainment directorate under the first Trump administration.

Greg Barbaccia: Serving as the federal chief information officer within the Office of Management and Budget. Previously held several roles in blockchain companies and as a CISO at a technology company focused on using artificial intelligence.

Cyber Threat Landscape



February

U.S. Government Advisory on **Volt Typhoon**

Ransomware Attack on Healthcare Payment Processor

May

Ransomware Attack on Hospital System

June

Ransomware Attack on Auto Sales/Service Software Provider

August

Ransomware Attack on Port Authority

October

U.S. Government Advisory on **Salt Typhoon**

November

Ransomware Attack on Logistics/Supply Chain Provider

Shift in Priorities

The Biden administration emphasized establishing minimum cybersecurity requirements for critical infrastructure. The Trump administration has shifted focus toward deregulation, risk-based resilience, and reinforcing national security through deterrence.

Biden Administration	Trump Administration
Sector-by-sector baseline cybersecurity requirements	Risk-based approach to critical infrastructure protection
Using the "power of the purse" to drive cybersecurity market	Deregulatory focus and promotion of innovation
National security focus on international coalitions – Counter Ransomware Initiative	National security focus on offensive cyber operations and deterrence

Looking Forward – Key Rules

- **Cyber Incident Reporting for Critical Infrastructure Act of 2002**: Requires infrastructure companies to confidentially report cyber attacks within three days and report ransom payments within 24 hours. *(Rulemaking ongoing)*

- **SEC Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rule**: Requires publicly traded companies to disclose material cybersecurity incidents within four business days absent a national security waiver from the attorney general and requires companies to report their cyber risk management, strategy, and governance practices. (*Effective as of December 2023)*

- **Health Insurance Portability and Accountability Act Security Rule:** Updates current rule to remove the distinction between "required" and "addressable" implementation specifications; requires specific controls, including multi-factor authentication, network segmentation, and vulnerability scanning/penetration testing. *(Rulemaking ongoing)*

Key Congressional Cyber Policy Areas

Cyber Information Sharing Act of 2015 Reauthorization: Safeguards for companies that voluntarily share cyber threat intelligence data with the government or each other, such as federal antitrust exemptions and shields against state and federal disclosure laws. *(Sunsets September 30, 2025)*

Regulatory Harmonization: Reintroduction of legislation focused on reducing duplication and redundancies in cybersecurity regulatory and administrative requirements – eye to reciprocity?

State and Local Cybersecurity Grant Program: Congress is debating the approach to continuing to fund and improve state and local cybersecurity. The current SLCGP is set to expire at the end of September 2025. From a recent hearing: “*The Federal government must continue to support and strengthen cybersecurity at the state and local levels to protect our nation’s networks and critical infrastructure.*”

Cyber Policy in Europe

Last year, the EU Commission said “no new cyber acts” in the 2025-29 term. That belies the scope of activity:

Implementation of Cyber Resilience Act (digital products)

Implementation of NIS2 Directive (critical infrastructure)

Implementation DORA (financial services)

Implementation of the Cyber Solidarity Act (cyber preparedness)

Cyber Security Act review (certification schemes and ENISA resourcing)

- Existing cybersecurity certification schemes – EUCC, EUCS, EU5G, Managed Service Providers

A raft of proposals to enhance digital sovereignty – Protect EU, Digital Workplan, Sovereign Cloud

Cyber Policy in the Rest of the World

United Kingdom:

- Cyber Security Resilience Bill (critical infrastructure)
- Proposal ban on ransomware payments
- Proposal on data brokers and national security
- Secure Software Development Code of Practice
- AI Cyber Security Code of Practice

Japan: Active Cyber Defense Bill

Australia: 2023-2030 Cyber Security Strategy

- SOCI Act (critical infrastructure)
- Ransomware and incident reporting
- Horizon 2 (2026-2028)

Regulatory Cooperation – Definition

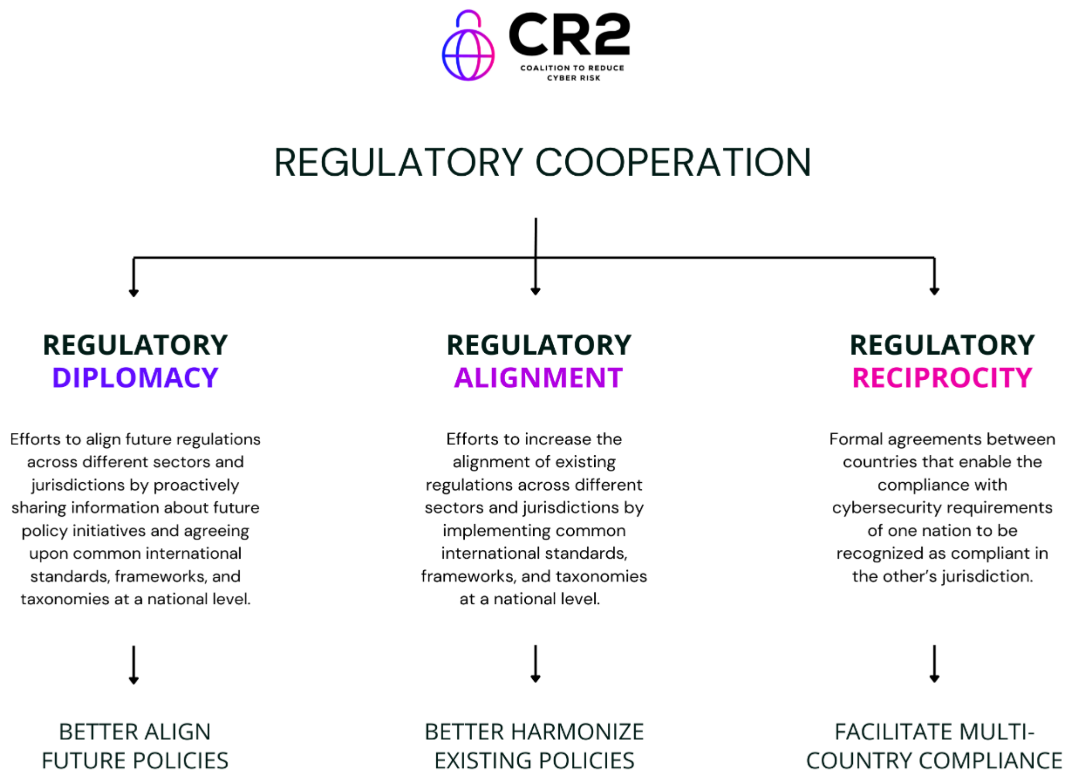
100 of 194 UN member states have defined critical infrastructure sectors.

Each has its own:

- Definition of who is in scope
- Requirements of those in scope
- Incident reporting thresholds & timelines
- Etc.

This is just one area of cyber policy divergence.

We need more international alignment of cyber policies!



CR2
COALITION TO REDUCE CYBER RISK

REGULATORY COOPERATION

REGULATORY DIPLOMACY

Efforts to align future regulations across different sectors and jurisdictions by proactively sharing information about future policy initiatives and agreeing upon common international standards, frameworks, and taxonomies at a national level.

BETTER ALIGN FUTURE POLICIES

REGULATORY ALIGNMENT

Efforts to increase the alignment of existing regulations across different sectors and jurisdictions by implementing common international standards, frameworks, and taxonomies at a national level.

BETTER HARMONIZE EXISTING POLICIES

REGULATORY RECIPROCITY

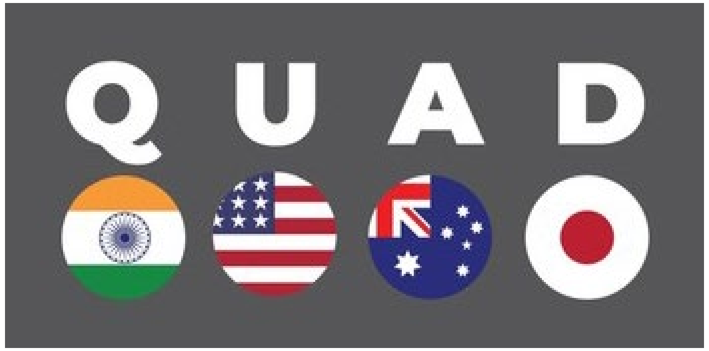
Formal agreements between countries that enable the compliance with cybersecurity requirements of one nation to be recognized as compliant in the other's jurisdiction.

FACILITATE MULTI-COUNTRY COMPLIANCE

Regulatory Cooperation – Policy Focus

Topic	Regulatory Cooperation Initiative	Industry Priority	Harmonization Feasibility	Reciprocity Feasibility
Critical Infrastructure Cybersecurity	Alignment of security measures requirements	High	Medium	■
	Transition to Post-Quantum Cryptography (PQC)	Medium	High	■
Critical Infrastructure Cybersecurity	Labelling – mutual recognition of national labels	Medium	■	High
	Mutual recognition of conformity assessment for cybersecurity labels	Medium	■	High
Incident Reporting	Reportable incident thresholds	High	Medium	Low
	Alignment of what information is to be reported	High	Medium	High
Ransomware Reporting	Alignment of what information is to be reported	Low	Medium	High
Secure Software Development	Alignment of security measures/best practices	High	Medium	Low
	Common attestation form/ mutual recognition	High	■	Medium

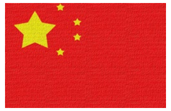
Regulatory Cooperation – Forums



Geopolitical Backdrop – Key Drivers

U.S. wants to promote an America First agenda

Europe wants domestic digital sovereignty



China wants growing exports of technology products and services

Asia (ex-China) wants certainty on security and trade

How do these drivers fit together?

Join Our Next Transition Outlook Webinar

April 16, 2025: The First 100 Days of the Second Trump Administration: A Policy and Regulatory Retrospective | 2:00 - 3:00 p.m. ET

Join us next Wednesday, April 16, for a discussion of the first 100 days of the second Trump administration. This webinar will take stock of the administration's early actions and emerging priorities across key policy and regulatory areas. It will explore executive orders, personnel decisions, agency direction, and early legislative activity to help make sense of where the administration is headed—and what it all means for businesses and organizations.

This document is published by the law firm Venable LLP. It is not intended to provide legal advice or opinion. Such advice may only be given when related to specific fact situations that Venable has accepted an engagement as counsel to address.

VENABLE LLP