Cybersecurity
2025 Preview

CAPSTONE

Firewall Frenzy:
Cyber Vendors Benefit Amid Rising Global Tensions

THE BOTTOM LINE

We believe the Trump administration will take a more aggressive cyber-security posture and gut the Cybersecurity and Infrastructure Security Agency (CISA)—moves that will escalate global cybersecurity tension. We also expect Congress to push for cyber regulation harmonization and modernization, creating tailwinds for cybersecurity vendors and consultants and headwinds for telecom, pipelines, and utility critical infrastructure.

Outlook at a Glance

- GROWING APPETITE FROM CONGRESS AND THE TRUMP ADMINISTRATION FOR CYBER MODERNIZATION, A POSITIVE FOR SOFTWARE PROCUREMENT AND LICENSING REFORM
- TRUMP TO SHIFT TOWARD OFFENSIVE CYBER POSTURE, INCREASING DEFENSE AND INTELLIGENCE COMMUNITY CYBERSECURITY SPENDING, A POSITIVE FOR DEFENSE-ORIENTED CYBER FIRMS
- TRUMP TO REDUCE CYBERSECURITY AND INFORMATION SECURITY AGENCY (CISA)'S FUNDING AND AUTHORITY; NATION-STATE AND RANSOMWARE ATTACKS ON CRITICAL INFRASTRUCTURE TO INCREASE
- CONGRESS TO PURSUE CYBER REGULATION HARMONIZATION WITH TRUMP ADMINISTRATION SUPPORT, A POSITIVE FOR CYBER-IMPLEMENTATION CONSULTANTS

Growing Appetite from Congress and Trump Administration for Cyber Modernization, a Positive for Software Procurement and Licensing Reform

Winners	Palo Alto Networks (PANW), Crowdstrike (CRWD), SentinelOne (S), Fortinet (FTNT), Accenture Plc (CAN), Booz Allen Hamilton (BAH), Leidos Holdings Inc (LDOS)
Losers	Broadcom Inc (AVGO), Hewlett Packard Enterprise Co (HPE), SolarWinds (SWI)

Capstone believes Congress and the incoming Trump administration will look to resolve inefficiencies in the current federal software procurement system, attempting to modernize federal agencies' tech stacks in the process. We anticipate this overhaul will create an opportunity for cutting-edge cybersecurity tech stack providers to increase their federal footprint. On December 4, 2024, the House passed the Strengthening Agency Management and Oversight of Software Assets Act (SAMOSA Act). The bill would require the Chief Information Officers (CIOs) of all federal agencies to conduct a full inventory and assessment of current software use for their agency and a strategy to consolidate software licenses by adopting enterprise software license agreements by software category. The bill also requires agencies to create software modernization plans for their respective agencies. A companion bill, introduced by Senators Gary Peters (D-MI) and Bill Cassidy (R-LA), was approved by the Senate Homeland Security and Governmental Affairs Committee in May 2023 but has yet to make it to the Senate floor.

Congress has looked to the incoming administration for support in this effort. Senator Joni Ernst (R-Iowa) launched a Department of Government Efficiency (DOGE) caucus on November 22, 2024, and included consolidating federal software licenses in a list of cost-cutting ideas she sent to Elon Musk and Vivek Ramaswamy, the heads of DOGE, citing a potential $750 million in savings from a 2023 study backing the SAMOSA Act.

Capstone anticipates that the Trump administration, including DOGE, will support congressional efforts to rehaul IT procurement and use the change to push for their vision for modernization. Vivek Ramaswamy recently told the Aspen Security Forum that DOGE will prioritize removing the federal government's data silos and improving its tech stack because he believes the government's legacy IT systems are major barriers to executing on DOGE's mission and plans of leveraging AI to identify areas of inefficiency. To remove data silos, we believe the government would also have to push agencies toward uniform cybersecurity solutions and tools.

We believe the Trump administration will additionally pursue administrative paths to modernize the government's cybersecurity tech stack and find cost efficiencies. Currently, each federal agency is responsible for procuring its own cybersecurity solutions. Many leverage the Continuous Diagnostics and Mitigation (CDM) program, which streamlines cybersecurity procurement for federal agencies by managing an Approved Products List (APL) and Blanket Purchase Agreements (BPA) that cover approved vendors and implementation consultants. In our view, the incoming administration would likely expand this model, running a competitive process to select a default cybersecurity tech stack to be adopted by agencies.

We expect another possible avenue for the Trump administration to overhaul its cybersecurity approach, which will be expanding cybersecurity requirements for federal agencies beyond the capabilities of legacy providers, prompting a new stream of procurement and replacement of current systems. One possible path to this outcome is for the White House Office of Management and Budget (OMB) to expand agency security requirements to include Extended Detection and Response (XDR) solutions and more advanced AI cybersecurity tools. Under Executive Order (EO) 14028, Improving the Nation's Cybersecurity, the Biden administration took significant steps toward ensuring a baseline of cybersecurity across federal agencies, including mandating the Federal government adopt a zero trust architecture and Endpoint Detection and Response (EDR) solutions.

Trump to Shift Toward Offensive Cyber Posture, Increasing Defense and Intelligence Community Cybersecurity Spending, A Positive for Defense-Oriented Cyber Firms

Winners	Palantir Technologies Inc (PLTR), C3.ai Inc (AI), Leidos Holding Inc (LDOS), Booz Allen Hamilton (BAH), Shield AI
Losers	Critical infrastructure companies

Capstone believes the incoming Trump administration will prioritize an offensive cyber strategy and allocate additional resources to cyber operations under the Department of Defense (DoD) and the Intelligence Community (IC) and cyber defense for state and local governments. We believe this effort will include expanding DoD AI capabilities. Trump's election platform includes a point to use "all the tools of National Power" to protect critical infrastructure and the industrial base from cyber actors. Under the first Trump presidency, the 2018 DoD Cyber Strategy introduced a core mission of "defend[ing] forward' to U.S. cyber operations, meaning a preemptive rather than reactionary response to cyber-attacks. We believe Trump will expand and extend his first-term policy to an offensive, hybrid approach to cybersecurity, potentially including kinetic efforts to dismantle cyber operations.

Capstone expects Trump's offensive cyber efforts will be directed against state-supported actors in China, Iran, and potentially Russia. Microsoft's Brad Smith recently urged Trump to "push harder" against the three countries. CISA has recently attributed hacks during the elections to both countries, including China's attempted hack of Trump and JD Vance's phones via Verizon and Iran's hack of the Trump campaign. Although we believe an offensive cyber approach will effectively deter major cyber-attacks, we anticipate the short-term effect will be an escalatory environment, including preemptive and retaliatory attacks from adversarial states and state-sponsored cybercrime groups. In our view, these attacks will continue to focus on critical infrastructure, creating high costs for incident response and potential ransomware payouts for affected critical infrastructure companies and increasing spending on cybersecurity and cyber incident insurance for the sector.

Trump to Reduce Cybersecurity and Information Security Agency (CISA)'s Funding and Authority; Nation-state and Ransomware Attacks on Critical Infrastructure to Increase

Winners	Palo Alto Networks (PANW), Crowdstrike (CRWD), SentinelOne (S), Fortinet (FTNT), Rapid7, (RPD), CyberArk Software (CYBR)
Losers	Critical infrastructure companies, most notably in the telecom, pipeline, and utility industries

Capstone believes the Cybersecurity and Infrastructure Security Agency (CISA) will be targeted for cuts by the incoming Trump administration due to Republican criticism of its role in combatting mis- and dis-information and expansion of its budget. We expect hostile states and ransomware groups to be emboldened by a defunding of CISA, increasing the number of attempted and successful attacks on critical infrastructure and state and local governments, including at least one attack on the magnitude of the Colonial Pipeline ransomware attack. We expect critical infrastructure companies to double down on cybersecurity spending in response. In the medium-to-long term, we anticipate that Trump's offensive approach to cybersecurity will effectively deter major attacks on critical infrastructure.

CISA was originally created in Trump's first term but started to draw criticism from Trump when Chris Krebs, CISA's first director, came out refuting Trump's claims of voter fraud in late 2020. CISA has since drawn the ire of the right due to its incorporation of a team to fight mis-, dis-, and malinformation (MDM) online. In June 2023, the House Select Subcommittee on the Weaponization of the Federal Government came out with a report on "The Weaponization of CISA," alleging CISA colluded with big tech companies to censor U.S. citizens. Critics on the right argue this is a significant divergence from CISA's original mandate to protect federal civilian and critical infrastructure.

Although Sen. Rand Paul (R-KY) would prefer to eliminate the agency, we expect its budget will instead be significantly cut and the rulemaking

and oversight role diminished. Since its creation in 2018, the agency's budget has increased from approximately $2 billion to $3 billion across 3,641 FTEs. Project 2025 calls for the Department of Homeland Security to be dismantled and for CISA to be moved under the Department of Transportation accordingly. Project 2025 also calls for CISA to limit its involvement in election security beyond cyber hygiene assessment for states and localities and to not duplicate the cybersecurity functions of the DoD, FBI, National Security Agency (NSA), and U.S. Secret Service.

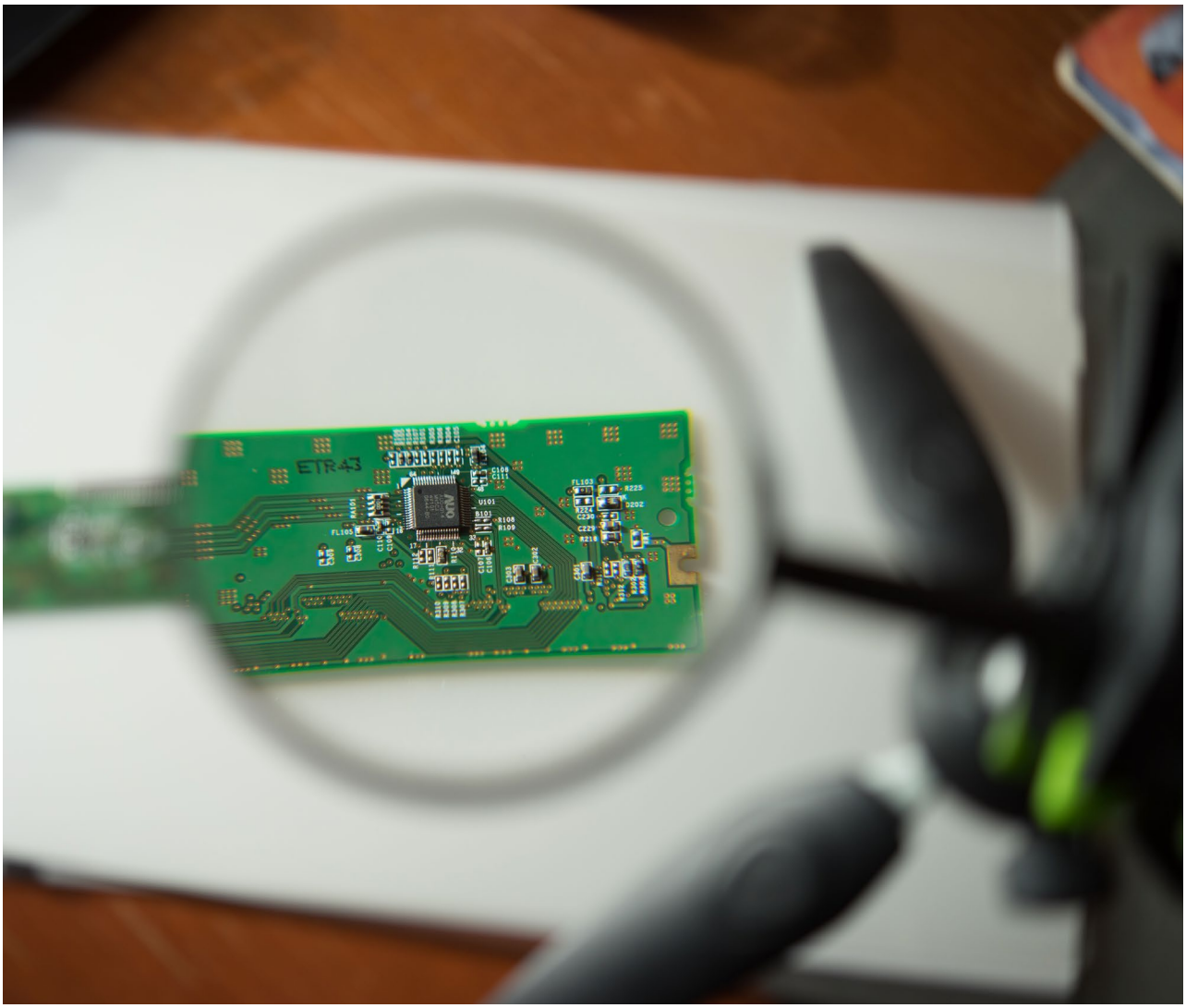
We believe CISA's regulatory role will be diminished under the Trump administration. CISA is not a regulator and has no enforcement or punitive capabilities, but the Biden administration has tasked it with creating regulations for the critical infrastructure sector, including, but not limited to, rulemaking under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). We expect the incoming administration to view CISA's role in regulatory rulemaking as one of its areas of duplicative responsibility and shift its function to other agencies as part of harmonization efforts.

Congress to Pursue Cyber Regulation Harmonization with Trump Administration Support, a Positive for Cyber-Implementation Consultants

Winners	Booz Allen Hamilton (BAH), Cognizant Technology Solutions Corp (CTSH), DXC Technology (DXC), Critical infrastructure companies
Losers	N/A

Capstone expects Congress to continue pushing to streamline cybersecurity regulation because it is a bipartisan issue with strong private-sector support. We anticipate regulatory harmonization would free up funds spent on compliance so that the private sector can invest in cybersecurity in the heightened cyber threat environment. We believe cybersecurity harmonization bills will enjoy the incoming administration's support if reintroduced in the new Congress. In the past five years, as major cyber incidents like Colonial Pipeline in 2021 have highlighted the need for improved cybersecurity across industries, regulatory bodies across state, national, and international governments have rushed to implement cybersecurity regulations, rarely with any level of coordination, creating a patchwork of duplicative and conflicting requirements that have become increasingly difficult and costly to navigate.

In July, Senators Gary Peters (D-MI) and James Lankford (R-OK) introduced the Streamlining Federal Cybersecurity Regulations Act, which



aims to address “harmonize” federal cybersecurity regulation by creating a committee of the National Cyber Director and all regulatory agencies to create a new streamlined regulatory framework within one year. The bill has made it out of the Homeland Security and Government Affairs committee but has not yet been brought to the floor. A partner bill was introduced in the House in November. If the bill passes, we expect DOGE to be included in the committee established by the act.

We believe private-sector demand for harmonization will create a continued incentive and pressure for Congress and the incoming administration to prioritize the issue. In June 2024, the Office of the National Cyber Director (ONCD) published a summary of responses to their August 2023 Request for Information (RFI) on cybersecurity regulatory harmonization. The RFI gave a clear mandate from the private sector and state governments for the federal government to prioritize harmonization. The respondents made clear how burdensome regulations had become. As global spending on information security is projected to reach $212 billion in 2025, Chief Information Security Officers (CISOs) are spending 30-50% of their time on compliance. In tandem with the RFI summary, the ONCD announced its plan to launch a pilot reciprocity framework focused on critical infrastructure sub-sectors, but the National Cyber Director, Harry Coker, made it clear that the ONCD needs Congress’s assistance to implement and codify a baseline harmonization effort fully.

About Capstone

- Capstone is a global, policy-driven strategy firm helping corporations and investors navigate the local, national, and international policy and regulatory landscape.

Work with Us

We tailor our work to help our clients predict meaningful policy and regulatory backdrops, quantify their impact, and recommend strategies that unveil novel opportunities and avoid hidden risks.

Contact Us

To learn more about our products, services, and solutions, reach out to sales@capstonedc.com or visit our website at capstonedc.com.