NTSC
NATIONAL TECHNOLOGY SECURITY COALITION

YEAR IN REVIEW

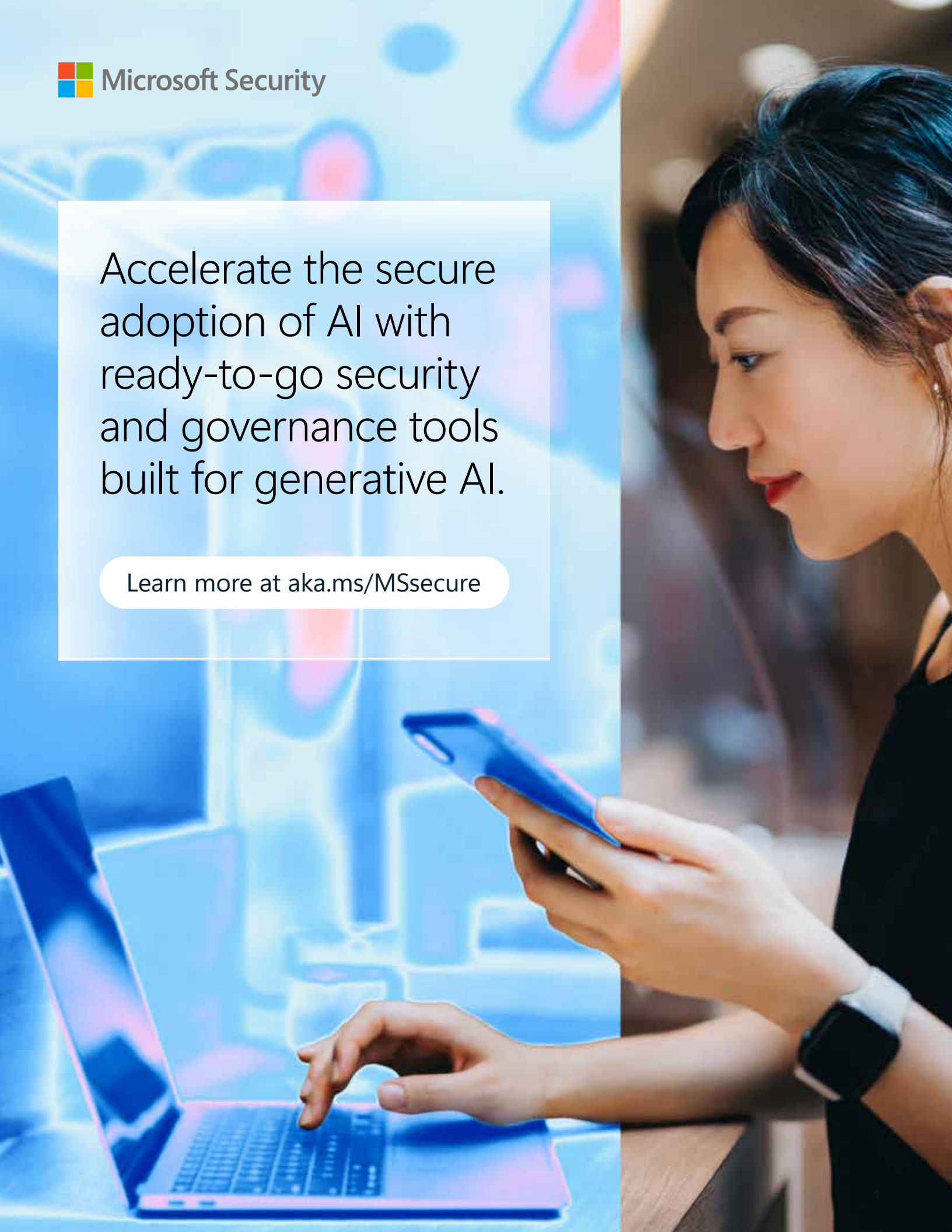
2024 Year End Report

CELEBRATING 10 YEARS
10
NATIONAL TECHNOLOGY SECURITY COALITION

Microsoft Security

Accelerate the secure adoption of AI with ready-to-go security and governance tools built for generative AI.

Learn more at aka.ms/MSsecure



2024 Year In Review

Table of **Contents**

Mission Statement

Through dialogue, education, and advocacy, the NTSC unites public and private leaders around national policies that improve national cybersecurity. As a non-profit, non-partisan organization, the NTSC serves as the preeminent advocacy voice of the CISO and brings US Government and industry cybersecurity leaders together to network and solve today's cybersecurity policy and collaboration challenges.

NTSC
NATIONAL TECHNOLOGY SECURITY COALITION

Letter from the **Chairman**

CELEBRATING 10 YEARS
NATIONAL TECHNOLOGY SECURITY COALITION
10

On one hand, it is hard to fathom that is has been 10 years – the time has gone by so fast. On the other hand, we have accomplished so much in building the organization that one might wonder how we did it in only 10 years.

Of course, the work to found the NTSC began before then. In late 2014, a few CISOs associated with the Technology Association of Georgia got together with the then-President and CEO of TAG. TAG was exploring ways to expand beyond Georgia and establish a national presence. The CISOs involved were looking for opportunities to influence national cyber policy – after all, CISOs must implement. The NTSC was born out of the merging of these two desires. We all agreed that we wanted to ensure we were non-profit, non-partisan, and not aligned to any particular industry. We wanted to stay focused on core principles that would benefit the nation and private organizations through a public-private partnership to protect against cyber security threats.

We had a clear vision of what we wanted to do – but not necessarily how to achieve it. TAG board members pitched in and helped refine the strategy and roadmap. The TAG president brought in an Executive Director because we needed someone with the time, focus and wherewithal to execute on the plan.

These past years have seen the growth of NTSC as the premier organization for the voice of the CISO on Capitol Hill. We have grown from 8 founding members to over 80 professionals across our board, partnerships, underwriters, Policy Council, and

We wanted to stay focused on core principles that would benefit the nation and private organizations through a public-private partnership to protect against cyber security threats.

> We have a fantastic future ahead of us.

supporting individuals. We have experienced recognition and credibility in Washington, both in Congress and with federal agencies like ONCD & CISA.

Our regional policy roundtables and National Policy Conference have become premier events. We have benefited from former and current public officials who have lent their wisdom and ideas on key priorities and effective advocacy. We hosted an impressive list of thought leaders and guest speakers, some of whom are named below.

- **Harry Coker,** National Cyber Director at ONCD
- **Lisa Einstein,** Chief AI Officer at CISA
- **Rear Admiral (Ret.) Mark Montgomery,** Senior Fellow at Foundation at Defense of Democracies (FDD)
- **Dr. Timothy Maurer,** Senior Director, Global Cybersecurity Advocacy at Microsoft Corporation
- **Dmitri Alperovitch,** Co-founder of CrowdStrike and Founder & CEO of Silverado Policy Accelerator
- **Christopher Isbrecht,** Head of Security Engineering at Check Point Software Technologies
- **Nicholas Leiserson,** Assistant National Cyber Director for Cyber Policy & Programs
- **Michael McGlynn,** Global CISO, World Wide Technology
- **Kelly Moan,** New York City CISO & Head of NYC Cyber Command
- **Andrew Scott,** Associate Director of China Operations at CISA

Our regional roundtables and national policy conferences are open to non-members. We find these forums to be a good way to introduce CISOs to NTSC. We also welcome partners who share an interest in contributing to strong national cyber policy.

Finally, on a personal note, I have been honored to serve the coalition these past 9 years. Together, we have had a major impact on the national landscape. We have seen many transitions in Congress and federal agencies due to elections and changes in administration. Because of the exemplary work of our members, we have been able to build new relationships with each transition. Our reputation of well-reasoned positions and non-partisan advice is recognized. Our thoughts and ideas are sought by policy makers. We have had a great past and I'm confident that NTSC will continue to grow in stature and as an organization. We have a fantastic future ahead of us. If you're on the fence about joining us in this quest, I would encourage you to get on board. It is a great ride.

Tim Callahan

Tim Callahan

Chairman of the Board
National Technology
Security Coalition

Letter from the **President**

> Our commitment to strengthening the public-private partnerships has never been stronger.

The rapidly evolving landscape of AI, quantum computing, and privacy technologies underscores the critical importance of our work.

As we begin 2025, during which we will celebrate our 10th Anniversary, I would like to reflect on our journey and outline our achievements and discuss what we have planned for the year ahead.

2024 has brought unprecedented advancements in technology and cybersecurity. Tools like generative AI have become increasingly integrated into daily applications, enhancing productivity and efficiency across industries. As well as AI and machine learning tools, quantum computing has also improved by leaps and bounds. Google's own quantum computer, Willow, demonstrated unprecedented computational power, solving complex problems in minutes that would take traditional supercomputers billions of years. Privacy-enhancing technologies are also advanced, offering innovative solutions like homomorphic encryption and differential privacy to protect personal information while enabling data analysis.

With all these rapid changes, the regulatory landscape also continued to shift, with new cybersecurity regulations and reporting requirements emerging across sectors. While we've witnessed this dramatic evolution reshape our digital landscape and bring both extraordinary potential and serious responsibilities, our commitment to strengthening the public-private partnerships has never been stronger, with the NTSC continuing to maintain ongoing open dialogues with congressional leaders, close collaboration with agencies like CISA and ONCD, and growing relationships with fellow technology think tanks and policy institutes which we hope to continue through the next year.

During 2024 the NTSC engaged in nearly 100 congressional meetings with key stakeholders who directly influence cyber policy legislation including the Senate and House Committees on Homeland Security, Commerce, and Intelligence. We provided expert witnesses at Congressional Hearings focused on Privacy and briefed ONCD and the Subcommittee on Cybersecurity within the House Homeland Security Committee on the need for cyber regulatory harmonization. We also hosted the National Cyber Director during one of his visits to Atlanta for a private meeting with a select group of executives from both the cyber and academic community.

We finished the year with 75 members across our board, policy and advisory councils representing a cross section of industries and providing voices from across the nation who invest their time and energy in ensuring a strong public/private

partnership continues to thrive. We added a number of new board members during the year including:

- **Cindi Carter,** Check Point Software Technologies
- **Mike Wagner,** Kenvue
- **Jason DeVoe,** Voya Financial
- **Tim Byrd,** M&T Bank
- **Brian Fricke,** City National Bank of Florida
- **Stephen Ford,** Rockwell Automation
- **Dan Sadler,** Constellation Energy

We also had some exciting shifts in leadership for our members during the last year, including Stacy Hughes moving from Voya Financial to ABM Industries, Shaun Khalfan moving from Discover Financial Services to PayPal, Jason Witty from USAA to Fidelity Investments, Kate Kuehn from AON to World Wide Technology, Donna Kidwell from Arizona State University to the University of Toronto and Darren Highfill made the jump to Accenture from Norfolk Southern.

Throughout the year, the NTSC hosted regional roundtables in St. Louis. Washington, D.C. and New York City. In July we hosted our national policy conference in Washington, D.C. with an impressive list of guest speakers. These events are designed to provide our members and guest speakers with an opportunity to express their views on the issues that matter most to the cyber community, ensuring the positions taken by the NTSC truly represent the national voice of the Chief Information Security Officer during our meetings across the nation.

It is with great pride and heartfelt appreciation that we also recognize the exceptional contributions of several individuals who have been instrumental in the success and growth of the NTSC not just over the last years but some, decades. Their unwavering commitment and expertise have truly elevated our organization to new heights. Tim Callahan, whose leadership as Board Chair since 2016 has been nothing short of exemplary with his global advocacy and willingness to provide counsel, despite his demanding role at Aflac, have been invaluable. A special salute also to Don Boian for his tireless dedication in chairing the Strategic Directions Committee until December 2024. His meticulous attention to detail and commitment to excellence has set a high standard for his successor. Robert Ball, whose astute guidance as Chair of the Policy Council has been crucial in shaping our legislative agenda.

These individuals exemplify the very best of our organization, and their contributions have been truly transformative. We are profoundly grateful for their service and look forward to continued success under their guidance.

As we look towards the future, the NTSC remains committed to its mission of fostering collaboration between public and private sectors to enhance national cybersecurity. Our achievements in 2024, despite occasional challenges, demonstrate the resilience and dedication of our members. The rapidly evolving landscape of AI, quantum computing, and privacy technologies underscores the critical importance of our work.

In 2025, we aim to expand our membership, strengthen our advocacy efforts, and continue to be at the forefront of cybersecurity policy discussions. With the support of our esteemed board members and the expertise of our diverse membership, we are well-positioned to navigate the complex cybersecurity challenges ahead. Together, we will continue to shape the future of national technology security, ensuring that our voice remains influential in the development of effective and practical cybersecurity policies.

As we embark on this new year, I extend my heartfelt gratitude to all our members, partners, and supporters. Your commitment and contributions are the driving force behind any success we obtain as an organization. It's an exciting time for our industry and I hope we all move forward with renewed vigor, ready to tackle the challenges of 2025 and beyond.

Larry Williams

President
National Technology
Security Coalition

Policy Update

Harmonizing Cyber Incident Reporting

When faced with a cybersecurity incident, CISOs must contend with more than just the threat itself. They must also contend with a myriad of state incident reporting regulations and proposed regulations on the federal level. These reporting regulations have differing standards on what qualifies as an incident, on what timeline incidents must be reported, and different processes for reporting said incidents. CISOs who fail to meet these various requirements may face legal penalties.

Amidst a cybersecurity incident, CISOs should be focused on responding to the attack, not running through an extensive list of reporting requirements for several different agencies. As such, the NTSC believes the best solution is for CISA to serve as the primary agency for all incident reporting requirements and as the only agency to which CISOs must report in the event of an incident. The Cyber Incident Reporting for Critical Infrastructure Act already designates CISA as the principal agency for critical infrastructure incident reporting. We would like to see that requirement expanded to cover all cyber incidents, not just those that impact critical infrastructure.

Moreover, we believe that incident reporting works best when CISA is a partner with the private sector rather than a regulatory body like the Federal Trade Commission. CISA has worked to foster a positive relationship with the private sector, and that relationship is key to effective incident reporting.

Securing the Software Supply Chain

Securing the software supply chain is essential to protecting critical systems from cyber adversaries who exploit vulnerabilities in third-party components, dependencies, or updates. A single compromise in the supply chain can cascade into widespread disruptions or breaches, making it vital for organizations to adopt proactive measures.

One effective approach is CISA's Secure by Design initiative, which emphasizes building security into software from the ground up rather than treating it as an afterthought. Integrating secure coding practices, rigorous testing, and transparent supply chain processes help ensure software is resilient to exploitation.

Secure by Design, combined with practices like dependency management, vendor scrutiny, and real-time monitoring, create a robust defense against emerging threats, protecting organizations and the ecosystems they support.

Advocating for Congressional Action on AI Regulation

Artificial intelligence (AI) is rapidly transforming every sector, from healthcare and education to national security and finance. While its potential to drive innovation and efficiency is undeniable, the technology's accelerated pace of development has outstripped existing regulatory frameworks. As AI becomes more powerful and pervasive, the risks of misuse, unintended consequences, and ethical dilemmas grow exponentially. Congress must step in to create guardrails that ensure AI is developed and deployed responsibly, safely, and equitably.

Secure by Design

Emphasizes building security into software from the ground up

Congressional Action

To establish the guardrails needed to harness AI's benefits

One pressing concern is the lack of transparency in how AI systems make decisions, often described as the "black box" problem. Without clear oversight, these systems could inadvertently embed biases, perpetuate inequalities, or make critical errors in high-stakes scenarios such as criminal justice, hiring, or autonomous vehicles. Congressional action is needed to mandate transparency, accountability, and fairness in AI algorithms to prevent harm and build public trust.

Additionally, AI poses significant national security risks. Adversarial nations and cybercriminals are increasingly leveraging AI for disinformation campaigns, cyberattacks, and espionage. The NTSC strongly encourages Congress to work with federal agencies like the Cybersecurity and Infrastructure Security Agency (CISA) to develop standards for securing AI systems against malicious exploitation.

Congress has a unique opportunity—and responsibility—to establish the guardrails needed to harness AI's benefits while addressing its challenges. Through thoughtful regulation, including measures to enforce transparency, bolster security, and promote ethical development, lawmakers can ensure AI serves as a force for good in society rather than a source of harm. Delays in action could result in unchecked risks, eroded public trust, and loss of global competitiveness. The time to act is now.

Securing the Nation's Critical Infrastructure

In a small control room nestled beneath a bustling city, operators monitor the nation's critical infrastructure—power grids, water systems, and communications networks—that keep daily life running smoothly. Yet behind this calm facade, a complex and persistent threat looms. Nation states, notably China with its sophisticated cyber capabilities, have repeatedly sought to exploit vulnerabilities in our systems. Alongside other adversaries, these foreign powers aim to disrupt, destabilize, and even undermine our national security.

This modern narrative of defense is not just about responding to isolated cyberattacks; it's a comprehensive call to action. The protection of critical infrastructure has become the frontline of our national security strategy. As technology evolves and interconnects every facet of our lives, so too do the methods employed by those who wish to see our systems fail. In this high-stakes environment, safeguarding our essential services means investing in robust cybersecurity, innovative technology, and coordinated defense strategies that can outpace the ever-evolving threats posed by state actors around the globe.Establishing a CISO Safe Harbor.

Creating a CISO Safe Harbor is a critical consideration in today's stringent cyber regulatory environment, where Chief Information Security Officers (CISOs) often face intense scrutiny during security breaches. The concept aims to provide CISOs with legal and professional protections, encouraging them to implement robust security measures without fear of undue personal liability.

The regulatory landscape has heightened expectations for CISOs to ensure compliance with evolving cybersecurity laws, such as SEC disclosure requirements and state-level data protection statutes. Additionally, recent high-profile breaches have spotlighted CISOs, raising concerns about individual accountability and liability.

A CISO Safe Harbor framework could offer protections for CISOs who demonstrate good-faith efforts to secure their organizations. These efforts might include implementing industry best practices, adhering to regulatory requirements, maintaining transparency in risk reporting, and aligning with frameworks like NIST or ISO. By codifying such protections, organizations and regulators can incentivize proactive cybersecurity leadership, ensuring that CISOs can focus on risk mitigation without the threat of disproportionate penalties.

This approach would foster a collaborative rather than punitive environment, encouraging CISOs to address cyber threats while mitigating personal risks associated with their role.

Board of Directors

Officers

- **Tim Callahan**—Aflac (Chair)
- **Jason Witty**—Fidelity Investments (Vice Chair)
- **Curley Henry** —The Southern Company (Vice Chair)
- **Larry Williams**—TAG (President)
- **Kristin Cornish**—The Coca Cola Company (Treasurer)
- **Michael Blache**—TaxSlayer (Secretary)

Board Members

- **Marene Allison**—Board Advisor
- **Geoff Aranoff**—GE Healthcare
- **Ben Aung**—The Sage Group
- **Mario Balakgie**—World Wide Technology
- **Michael Blache**—Tax Slayer
- **Beth-Anne Bygum**—Q2 Solutions
- **Timothy Byrd**—M&T Bank
- **Cindi Carter**—Check Point Software Technologies
- **Janet Cinfio**—Acxiom
- **Jason DeVoe**—Voya Financial
- **John Dunn**—Accuray
- **Jim Eckart**—Microsoft Corporation
- **Joe Ellis**—Ryder Systems, Inc.
- **Jamil Farshchi**—Equifax
- **Stephen Ford**—Rockwell Automation, Inc.
- **Brian Fricke**—City National Bank of Florida
- **Steve Fridakis**—Oracle Healthcare
- **John Gift**—Smurfit WestRock
- **Kevin Gowen**—Synovus
- **Stacey Halota**—Graham Holdings
- **Gary Harbison**—Johnson & Johnson
- **Shawn Harris**—Chipotle Mexican Grill
- **Wayne Hilt**—Huntington National Bank
- **Stacy Hughes**—ABM Industries
- **Shaun Khalfan**—PayPal
- **Katherine Kuehn**—CISO in Residence
- **David Lin**—CISO in Residence
- **Jacob Lorz**—Cintas
- **Dr. Adrian Mayers**—Premera Blue Cross
- **Kristen McCooey**—Edward Jones Investments
- **Lucia Milică**—Stanley Black & Decker
- **Allison Miller**—United Health Group/Optum
- **Benjamin Murphy**—Unum Group
- **David Nolan**—Aaron's
- **Michael Palmer**—Hearst
- **Steve Pugh**—InterContinental Exchange
- **Stephen Richardson**—Scientific Games
- **Ray Rothrock**—RedSeal, Inc.
- **Richard Rushing**—Motorola Mobility
- **Dan Sadler**—Constellation Energy
- **Forrest Smith**— Ingram Micro
- **Billy Spears**—Teradata
- **Brian Waeltz**—Cardinal Health
- **Michael Wagner**—Kenvue
- **Steven Weber**—AbbVie
- **Reginald Williams**—The Chemours Company
- **Saša Zdjelar**—ReversingLabs

New Members 2024

Tim Byrd
M&T Bank

Cindi Carter
Check Point Software Technologies

Jason DeVoe
Voya Financial

Stephen Ford
Rockwell Automation, Inc.

Brian Fricke
City National Bank of Florida

John Gift
Smurfit WestRock

Michael Wagner
Kenvue

The Industry's Best Prevention Rate

99.9%

Miercom

Miercom Enterprise and Hybrid Mesh Firewall Benchmark 2025

AI-Driven Threat Prevention.
That's **Security in Action.**

checkpoint.com/action

CHECK POINT™

Programming

2024 Events

In 2024 we hosted regional policy roundtables in St. Louis, Missouri in January, Washington, D.C. in March, and New York City in May. We also hosted our National CISO Policy Conference in Washington, D.C., in July. Additionally, we hosted virtual webinars with Rear Admiral (Ret.) Mark Montgomery, Senior Director of CCTI and Senior Fellow at Foundation for Defense of Democracies (FDD) and Executive Director of CyberSolarium.org and Lisa Einstein, Chief AI Officer at the Cybersecurity & Infrastructure Security Agency (CISA).

In 2024 we focused on five policy priorities:

- **Software Supply Chain Security**
  - Secure by Design
  - Secure by Default
- **Establishing a Federal Privacy Mandate**
- **CISO Safe Harbor**
- **Critical Infrastructure (Focus on OT/IT Integration & Digital Transformation)**
- **Continuing to Strengthen the Public/Private Partnership**

Both our regional events and our national conference were designed to speak to our policy priorities as well as other leading issues such as establishing guardrails for artificial intelligence, improving cyber threat intelligence, combatting ransomware, assessing third party risk management, especially within the software supply chain, and the continuing onslaught of new cybersecurity regulations being adopted by various federal agencies.

We heard from multiple speakers during the year including:

- **Harry Coker,** National Cyber Director at ONCD
- **Lisa Einstein,** Chief AI Officer at **CISA**
- **Rear Admiral (Ret.) Mark Montgomery,** Senior Fellow at Foundation at Defense of Democracies (FDD)
- **Dr. Timothy Maurer,** Senior Director, Global Cybersecurity Advocacy at Microsoft Corporation
- **Dmitri Alperovitch,** Co-founder of CrowdStrike and Founder & CEO of Silverado Policy Accelerator
- **Christopher Isbrecht,** Head of Security Engineering at Check Point Software Technologies
- **Nicholas Leiserson,** Assistant National Cyber Director for Cyber Policy & Programs at **ONCD**
- **Michael McGlynn,** Global CISO, World Wide Technology
- **Kelly Moan,** New York City CISO & Head of NYC Cyber Command
- **Andrew Scott,** Associate Director of China Operations at CISA

Our programming provides our members and select guests with an opportunity to have candid conversations with key players including members of congress, either on our legislative day, or by joining the NTSC Executive Director during one of his many trips to D.C.

In 2024 the NTSC, in partnership with The Reserve Component, our full-time representative in D.C., was able to meet with 80+ congressional offices throughout the year, sometimes to simply introduce the NTSC, and more often to discuss our policy priorities, specially our efforts to drive towards a national privacy mandate, which took many twists and turns throughout the year with the Introduction of the American Privacy Rights Act (APRA), which was unfortunately tabled at the last minute before dropping on the House Floor due to concerns with certain aspects of the bill on both sides of the House. However, the NTSC was invited to appear at a Hearing on the bill and Katherine Kuehn, NTSC Board Member and Area Vice President of Global Cyber Advocacy at World Wide Technology appeared on behalf of the NTSC to provide our perspective on the need for a national privacy mandate.

The NTSC also provided briefings to the Office of the National Cyber Director as well as key staffers on the Subcommittee for Cybersecurity within the House Homeland Security Committee on the need for harmonizing the cyber regulatory environment. In both cases, the NTSC was invited to provide these briefings and a number of our board members participated in these briefing sessions.

Cyber Threat
Landscape

In 2024, cyberattacks against the United States escalated in both frequency and sophistication, particularly from state-sponsored actors in Russia and China. These cyber adversaries have targeted critical infrastructure—power grids, water systems, transportation networks, and communication systems—posing significant threats to national security and economic stability.

China's cyber operations have been notably aggressive, with Volt Typhoon standing out as a particularly alarming campaign. This state-backed operation specializes in stealthy, long-term cyber espionage, infiltrating critical infrastructure networks and maintaining persistence for potential future disruption. Unlike traditional malware that steals data or causes immediate damage, Volt Typhoon focuses on pre-positioning itself within systems, effectively creating a "sleeper cell" in cyberspace. This tactic raises grave concerns about China's ability to disable vital services in times of geopolitical conflict. Similarly, Salt Typhoon, another Chinese-backed cyber threat group, has been linked to widespread espionage efforts against government agencies and defense contractors, seeking to exfiltrate sensitive military and technological intelligence.

Meanwhile, Russia continues to execute sophisticated cyber campaigns aimed at destabilizing the U.S. and its allies. The NotPetya malware attack, originally designed to target Ukrainian infrastructure, quickly spread worldwide, causing billions of dollars in damage, including to U.S. companies. More recently, Russian threat actors have been tied to attacks on energy grids and financial institutions, using ransomware and wiper malware to disrupt operations. Groups such as Sandworm, known for their role in the cyber takedown of Ukraine's power grid, have demonstrated capabilities that could be leveraged against the U.S. in future conflicts.

The increasing reliance on digital infrastructure makes these cyber threats even more dangerous. An attack on power grids or water treatment facilities could lead to cascading failures, endangering public safety and national security. As China and Russia continue to refine their offensive cyber capabilities, the U.S. must bolster its cyber defenses, enhance threat intelligence sharing, and develop proactive strategies to mitigate the risk of large-scale disruptions.

The increasing reliance on digital infrastructure makes these cyber threats even more dangerous.

In 2024 we witnessed a barrage of cyber-attacks across the board, from attacks on American businesses to our critical infrastructure with terms like Volt Typhoon, Salt Typhoon, and cyber threats loom large, and the digital landscape continues to evolve rapidly, which makes the collaboration between public and private entities a crit-ical ingredient in fortifying cyber defenses. This symbiotic relationship not only enhances operational effectiveness but also fosters a robust political environment conducive to addressing the complex challenges of cybersecurity.

Partnering

The need for a robust public-private partnership in cybersecurity has never been greater.

In an era where cyber threats are increasingly sophisticated and state-sponsored attacks pose significant risks to national security, the need for a robust public-private partnership in cybersecurity has never been greater. The United States' critical infrastructure—power grids, financial institutions, transportation systems, and healthcare networks—is largely owned and operated by the private sector. At the same time, nation-state actors, cybercriminals, and hacktivist groups relentlessly target these essential services. The only way to effectively defend against these threats is through a unified front—a strategic partnership between government agencies and private industry.

The Office of the National Cyber Director (ONCD) and the Cybersecurity and Infrastructure Security Agency (CISA) play pivotal roles in facilitating this collaboration. The ONCD sets national cybersecurity strategy and policy, ensuring that government efforts align with private sector needs. Meanwhile, CISA serves as the nation's risk advisor, providing threat intelligence, guidance, and resources to help businesses fortify their defenses against cyber threats.

01

WORK CLOSELY WITH FEDERAL AGENCIES

Including CISA and the Office of the National Cyber Director

02

MEET REGULARLY WITH CONGRESSIONAL OFFICES

Which impact our key legislative and policy priorities and shape legislation

Without seamless communication and intelligence sharing, the private sector remains vulnerable to attacks that could disrupt entire industries and national security. Government agencies often have access to classified intelligence on emerging threats, while private entities have real-time visibility into network vulnerabilities and cyber incidents. A structured partnership enables faster threat detection, coordinated incident response, and resilience-building strategies that benefit both sides.

Key initiatives like CISA's Joint Cyber Defense Collaborative (JCDC) and the ONCD's push for cybersecurity investment demonstrate the power of collaboration. However, there is still work to be done. Strengthening these partnerships means breaking down barriers to information sharing, increasing joint threat exercises, and ensuring a national cyber defense strategy that integrates both public and private resources.

As cyber threats from adversarial nations grow in complexity, the U.S. must prioritize a whole-of-nation approach to cybersecurity. Only by working together—government agencies, industry leaders, and technology innovators—can we build a resilient, secure digital ecosystem capable of withstanding the next wave of cyberattacks.

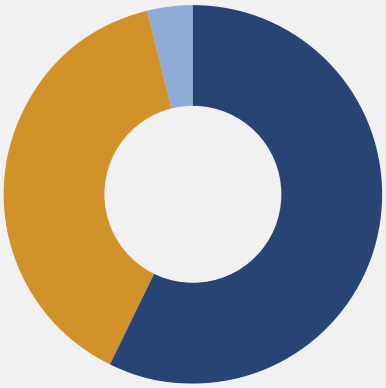
The NTSC has consistently listed the importance of continuing to strengthen public/private partnerships and we do this in several ways. First, we work closely with federal agencies including CISA, a relationship we have fostered since our earliest days. We have also continued to develop a strong working relationship with the Office of the National Cyber Director (ONCD) and ancillary organizations like the Foundation for the Defense of Democracies (FDD), the R Street Institute, and the Aspen

Cyber Institute; organizations that like the NTSC, have a vested interest in the defense of the nation against cyber adversaries, be they nation states or cyber criminals.

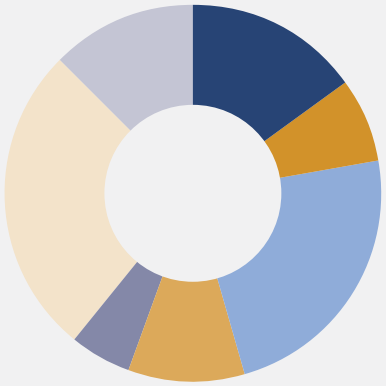
Second, we meet regularly with congressional offices that impact our key legislative and policy priorities and the committees that shape legislation such as the House Committee on Homeland Security, the House Committee on Energy & Commerce, the Senate Commerce Committee and many others. During the 118th Congress the NTSC participated in nearly 200 face-to-face meetings with congressional offices, both in the House and Senate.

One of the primary benefits of the public/private partnership is the exchange of threat intelligence. Our members possess invaluable insights into emerging cyber threats due to their visibility into vast networks of users and systems. Conversely, government agencies often have access to classified information and intelligence sources that can enrich the private sector's understanding of global cyber threats. Through collaboration, both parties can stay ahead of adversaries, proactively identifying vulnerabilities and deploying countermeasures to protect critical infrastructure and sensitive data, which was the motivation for the creation of the Joint Cyber Defense Collaborative (JCDC), an organization that unfortunately struggles to find its real identity, but we expect that to change in 2025 as JCDC is clearly on the agenda for the House Subcommittee on Cybersecurity.

Financial Overview



Member Fees	$ 478,690
Sponsorships	$ 325,000
Other Revenue	$ 31,084
Total Revenue	**$ 834,774**



Events	$ 110,177
Sales & Marketing	$ 54,609
Legal & Professional Fees	$ 170,979
Business Operations	$ 73,040
Travel	$ 38,649
Payroll	$ 195,030
Other Expenditures	$ 91,587
Total Expenditures:	**$ 712,093**
NET INCOME	**$102,733**

Legislative and Advocacy Update

Despite a tumultuous year in Congress characterized by slim majorities and political turmoil, the National Technology and Security Coalition (NTSC) and The Reserve Component (TRC) had a remarkably productive year advocating on behalf of CISOs. NTSC and TRC conducted nearly 100 meetings with cybersecurity leaders in Congress and the Administration. TRC also played a pivotal role in coordinating several key events on behalf of the NTSC, including securing speakers for the Annual National CISO Policy Conference. Additionally, TRC provided NTSC with a monthly report summarizing recent legislative and regulatory updates in the cybersecurity realm.

Slim majorities in both the House and Senate highlighted the need for bipartisanship, an area of expertise for NTSC. NTSC and TRC targeted congressional meetings with the Homeland Security Committees and the House AI Task Force where they advocated for several of NTSC's top priorities, including harmonizing cyber incident reporting, implementing a federal data privacy standard, prompting congressional action on artificial intelligence, and securing the software supply chain. Despite political upheaval, NTSC and TRC worked across party lines to raise awareness and gather congressional support for their cybersecurity priorities.

Thankfully, the uncertainty in Congress did not impede major cybersecurity policy developments, some of the most important of which are detailed below.

In January, CISA launched two training programs to bolster the cyber workforce and enhance diversity in the field. These free programs, the CyberSkills2Work and TryCyber, help adults and students begin careers in cybersecurity.

February was a busy month.

Firstly, the House of Representatives launched a bipartisan task force on artificial intelligence, aiming to foster the country's innovation while exploring regulatory measures that can mitigate risks presented by the technology. The task force is led by Chair Jay Obernolte (R-CA-23) and Co-Chair Ted Lieu (D-CA-36).

NTSC and TRC worked across party lines to raise awareness and gather congressional support for their cybersecurity priorities.

Secondly, House Republicans impeached Homeland Security Secretary Alejandro Mayorkas over concerns about the Biden Administration's handling of the U.S.-Mexico border. A vote of two-thirds of the Senate was required to remove Secretary Mayorkas from office, a threshold the Senate did not reach.

Finally, NIST released the long-awaited final version of the NIST Cybersecurity Framework (2.0). Notably, the new framework includes a new "govern" function, which defines executive leadership requirements in cybersecurity management.

In March, CISA published its long-awaited notice of proposed rulemaking (NPRM) for the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). The 447-page NPRM provides an overview of reporting requirements for covered entities. CISA collected feedback that will influence the final rulemaking, expected by September 2025.

Additionally, in March, the Federal Communication Commission voted to establish the Cyber Trust Mark cybersecurity labeling program for consumer Internet of Things products. The program incorporates requirements developed by NIST in collaboration with industry experts to extend its scope.

In April, President Biden issued a national security memorandum that formally designates CISA as the federal agency responsible for coordinating critical infrastructure security. The memorandum also directed DHS to submit a biennial national risk management plan and directed the U.S. intelligence agencies to collect and share information with critical infrastructure operators.

In April, NTSC Board Member and CISO-in-Residence Katherine Kuehn testified in front of the House Energy and Commerce Innovation, Data, and Commerce Subcommittee at a hearing titled "Legislative Solutions to Protect Kids Online and Ensure Americans' Data Privacy Rights."

In September, The Cyberspace Solarium Commission released its annual assessment, revealing that 80% of its 2020 cybersecurity recommendations have been implemented and outlined the top 10 policy recommendations for the incoming administration in 2025.

In December, Congress approved the fiscal 2025 NDAA, fully funding the $3.08 billion shortfall in the FCC's rip-and-replace program. Established in 2020, the program reimburses rural telecom providers for removing Huawei and ZTE equipment.

Additionally, in December, the House bipartisan Task Force on AI released their report after a year-long inquiry into potential innovation and risks of the technology. The report states that the federal government should adopt a structured and transparent approach to AI use by ensuring compliance with existing laws, improving workforce AI skills in hiring processes, enhancing cybersecurity and data governance, and supporting flexible governance and AI standards by reducing administrative burden, and maintaining high transparency standards.

NTSC will focus on advancing key cybersecurity priorities, including advocating for the harmonization of the cyber regulatory environment.

ADVOCACY FOCUS FOR 2025

A Look Ahead

The 2024 election brought significant changes to the 119th Congress. Republicans maintained control of the House by a slim margin of 218-215—the resignations of Reps. Matt Gaetz (R-FL-01) and Michael Waltz (R-FL-06) have spurred a special election scheduled for April 1, 2025. Republicans seized control of the Senate by flipping key seats in Montana, Ohio, Pennsylvania, and West Virginia. They currently lead with a margin of 53-47. Sen. John Thune (R-SD) was elected as Majority Leader in November. The Senate Homeland Security Committee is now chaired by Sen. Rand Paul (R-KY), and former Chair Sen. Gary Peters (D-MI) has assumed the position of Ranking Member. Sen. Peters also announced that he will retire at the end of his current term. Additionally, Kristi Noem has been confirmed as Secretary of Homeland Security.

In 2025, NTSC will focus on advancing key cybersecurity priorities, including advocating for the harmonization of the cyber regulatory environment. NTSC will continue to foster relationships with cyber veterans and newly elected members of Congress on Capitol Hill. Given the narrow margins in both chambers of Congress, NTSC and TRC believe that bipartisanship will continue to be the path forward.

THE CYBER CRISIS YOU'RE NOT PLANNING FOR

A cyberattack can take down your systems in minutes. A mishandled response can damage your brand for years.

CISOs who put communications at the center of their risk strategy weather the storm. Those who don't? Just ask the last company to go viral for all the wrong reasons.

We help tech leaders build a crisis plan before you need it. **Let's chat.**

Mike Neumeier, CEO
mneumeier@arketi.com
c 404.451.7832

arketi™ GROUP

www.arketi.com

NAVIGATING NEW PRIORITIES AND EMERGING TECHNOLOGIES IN 2025

The Future of Cybersecurity

As we progress through 2025, the cybersecurity landscape is undergoing significant transformations influenced by the current administration's policies, an evolving threat environment, and rapid advancements in technologies such as Artificial Intelligence (AI) and Quantum Computing.

Policy Shifts and Administrative Focus
The new administration has introduced pivotal changes in cybersecurity strategy. Notably, there has been a discernible shift in threat prioritization, with a reduced emphasis on Russian cyber threats. This change is evident from recent policy adjustments that downplay the cybersecurity risks associated with Russia, despite longstanding intelligence assessments highlighting such threats. This pivot has raised concerns among cybersecurity experts who argue that it may increase vulnerabilities to Russian cyber activities.

Concurrently, the administration is placing a heightened focus on countering cyber threats from China and Iran. This strategic realignment reflects broader geopolitical considerations and necessitates a recalibration of defensive measures to address the specific tactics employed by these nations.

Policy Shifts by New Administration

Discernible shift in threat prioritization, reducing emphasis on Russia

Evolving Threat Environment

Heightened focus on countering cyber threats from China and Iran

Advancements in Technology

AI and Quantum Computing is poised to revolutionize the industry

> The NTSC will continue to work with our partners, Congress and the relevant federal agencies to ensure the Voice of the CISO is not lost.

Advancements in AI and Quantum Computing

The rapid development of AI and Quantum Computing is poised to revolutionize both offensive and defensive aspects of cybersecurity.

Artificial Intelligence: AI is becoming integral to modern cybersecurity strategies, offering capabilities such as real-time threat detection and automated response mechanisms. However, adversaries are also leveraging AI to conduct more sophisticated and targeted attacks, necessitating the development of advanced AI-driven defense systems.

Quantum Computing: Presents a dual-edged sword for cybersecurity. On one hand, it holds the potential to break current cryptographic systems, rendering traditional encryption methods obsolete. On the other hand, it offers opportunities to develop new, quantum-resistant encryption techniques. The urgency to transition to quantum-safe cryptography is underscored by recent initiatives and reports highlighting the long-term risks posed by quantum computing to current cybersecurity infrastructures.

Strategic Initiatives and Future Outlook

To navigate these evolving challenges, several strategic initiatives are being emphasized:

Enhanced Public-Private Collaboration: Strengthening partnerships between government agencies and private sector entities is crucial for a unified defense against cyber threats. This collaboration facilitates effective information sharing and coordinated responses to incidents.

Investment in Emerging Technologies: Allocating resources toward the development of AI and quantum-resistant technologies is essential. Such investments aim to bolster defensive capabilities and mitigate the risks associated with technological advancements.

Comprehensive Policy Frameworks: Implementing robust cybersecurity policies that adapt to the dynamic threat landscape is imperative. These frameworks should address both current and emerging threats, ensuring a proactive rather than reactive stance.

The cybersecurity domain in 2025 is characterized by a complex interplay of shifting political priorities and technological innovations. Addressing these challenges requires a multifaceted approach that combines strategic policy decisions, technological advancements, and collaborative efforts across all sectors.

The NTSC will continue to work with our partners, Congress and the relevant federal agencies to ensure the Voice of the CISO is not lost as we progress through the year, and we encourage all of our members to continue to actively participate in the coalition to ensure your concerns and priorities are included in these conversations.

CELEBRATING 10 YEARS
10
NATIONAL TECHNOLOGY SECURITY COALITION

WE ENSURE THE CISO'S VOICE IS HEARD IN WASHINGTON, D.C.

The NTSC provides CISOs valuable opportunities to learn about national cybersecurity policy trends directly from cybersecurity leaders, policymakers, and national thought leaders while advocating for or against policies affecting our industry.

If you are interested in learning more about the NTSC, becoming a board member, or becoming an underwriter to support our efforts, contact:

Patrick Gaul, Executive Director
patrick@ntsc.org | 404.920.0703

NTSC
NATIONAL TECHNOLOGY SECURITY COALITION

World Wide Technology

Secure, all together

Blending business insight
with technical knowledge
to reduce overall risk.

Learn more on **wwt.com**

NTSC
NATIONAL TECHNOLOGY
SECURITY COALITION

Larry Williams
President, NTSC
LWilliams@tagonline.org
470.823.3546

Patrick Gaul
Executive Director, NTSC
Patrick@ntsc.org
404.920.0703

info@ntsc.org | **ntsc**.org