NTSC
NATIONAL TECHNOLOGY SECURITY COALITION

Year In Review

2023

Microsoft

Protect it all from end-to-end.

Learn more at www.microsoft.com

NTSC
NATIONAL TECHNOLOGY SECURITY COALITION

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.

2023 Year In Review

TABLE OF **CONTENTS**

LETTER FROM THE **PRESIDENT**

As we embark on a new year, it is my honor as the President of the NTSC to present our 2023 Year in Review.

This past year was marked by both challenges and triumphs. We faced a dynamic landscape of technological evolution with artificial intelligence advancing beyond what we would have imagined even a few years ago, creating both promises for the future as well as deep concerns for our welfare. We have seen an intricate web of cyber threats, data breaches, and emerging technologies, all requiring vigilance and adaptability by our members.

The regulatory landscape changed dramatically with the adoption of expanded cybersecurity regulations by the SEC fostering a new era of cyber enforcement. We are also seeing other government agencies pursue their own cyber incident reporting requirements fostering deep concerns for a future filled with competing cyber regulations causing confusion within corporate America.

But throughout the year, the NTSC continued to focus on our key policy priorities for 2023 including cyber incident reporting harmonization, establishing a federal privacy mandate, adopting a holistic approach to fixing the cyber workforce challenges, raising the bar on critical infrastructure – especially our most vulnerable assets including transportation, electricity and our water authorities – and finally continuing to strengthen the public/private partnership.

Your NTSC team regularly met with our congressional leaders and their staff, partnering with the Cybersecurity & Infrastructure Security Agency (CISA), the Office of the National Cyber Director (ONCD) and other like-minded organizations such as the Foundation for the Defense of Democracies (FDD), the Bipartisan Policy Institute, the R Street Institute and others.

The NTSC continued to grow in 2023 with several new members being added including:

- Kate Kuehn at AON
- Dr. Adrian Mayers at Premera Blue Cross
- Mario Balakgie at World Wide Technology
- Forrest Smith at Ingram Micro
- Jacob Lorz at Cintas
- Beth-Anne Bygum at Q2 Software
- John Dunn at Accuray
- Saša Zdjelar at Reversing Labs
- Billy Spears at Teradata
- Dave Lin at the Gemological Institute of America
- Ben Murphy at the UNUM Group
- Janet Cinfio at Acxiom
- Geoff Aranoff at GE HealthCare

However, as usually happens within our community, we saw some changes this past year with Beth-Anne Bygum leaving Acxiom to join Q2 and Janet Cinfio backfilling her seat on the board. John Dunn departed GE HealthCare to join Accuray, with Geoff Aranoff taking John's seat on the board. Bob Varnadoe moved to Kaiser Permanente and Paul Farley assumed the Corporate CISO role at NCR Voyix Corp, replacing Bob on the board.

We finished the year with 57 members against a target of 60; however, with Murray Kenyon (U.S. Bank) taking over as Chair of the Board Development Committee, we anticipate that we will continue to grow in 2024 and achieve our new target of 70 board members by December 31.

During 2023, the NTSC hosted regional roundtables in Washington, D.C., New York City, and Atlanta, as well as our national conference in Washington, D.C., which featured a fireside chat between CISA Director Jen Easterly and Microsoft Corporate Vice President Kelly Bissell along with a number of other respected guest speakers.

Patrick Gaul, our Executive Director, and I traveled to the UK to meet with a number of UK Government entities including the National Cyber Security Center (NCSC), and the Department of Science, Information and Technology (DSIT). We were hosted by Ben Aung, the Chief Risk Offcer at the Sage Group and Kate Kuehn, Chief Trust Officer at AON and we were joined by Seth Ryan, CEO of Collective Insights, a Platinum Underwriter for the NTSC.

Our goal was to begin to build the business case for UK expansion in 2025, aligned with the recommendations contained in the final report from PwC after they conducted a strategy refresh for the NTSC this past summer.

I would like to thank our Board Chair, Tim Callahan, for his amazing support, as well as our Executive Committee members including Jason Witty, our Vice Chair, Kristin Cornish, our Board Secretary, and Michael Blache, our Treasurer.

I would also like to recognize Don Boian, the Chair of our Strategic Directions Committee and all the members of that committee who have worked tirelessly this year to guide the organization towards becoming the National Voice of the CISO.

In closing, the reality is the challenges we will face in 2024 will undoubtedly persist and be exacerbated by the upcoming election cycle. But with dedication and the shared knowledge our members bring to the table, the NTSC is well positioned to continue to influence policy and legislation and represent our members in Washington, D.C. and beyond.

Thank you for your membership and your support throughout this past year.

Sincerely,

Larry Williams

President
National Technology
Security Coalition

POLICY UPDATE

Harmonizing Cyber Incident Reporting Requirements

The NTSC believes it is essential that we have one standard for cyber incident reporting, preferably following the guidelines articulated in the Department of Homeland Security's Cyber Incident Reporting Council report, *Harmonization of Cyber Incident Reporting to the Federal Government*, issued in September 2023. With federal agencies such as the Securities and Exchange Commission (SEC) issuing their own incident reporting requirements, and the impacts rules like the SEC's have had on CISOs, it remains critical that we continue to advocate for a single standard.

Continuing to Advocate for a Federal Privacy Mandate

In 2023 alone, twelve states signed into law or put into effect privacy legislation, and nine other states have introduced legislation. The NTSC believes that this privacy legislation patchwork is problematic for consumers and cybersecurity professionals alike. The federal government should develop a single, national privacy standard to ensure equal protection for consumers and easier requirements for cybersecurity professionals. To that end, in 2023, NTSC hosted staffers from the House Energy and Commerce Committee for a staff briefing in which CISOs educated staffers on the importance of privacy standards and the challenges they face with the state-led patchwork. Additionally, NTSC held dozens of meetings with members of the House Energy and Commerce and Senate Commerce committees to advocate for a federal mandate. NTSC will continue to meet with legislators and educate staff on the issue.

Establishing a Holistic, National Cyber Workforce Strategy

The Office of the National Cyber Director (ONCD) issued its *National Cyber Workforce and Education Strategy* in July 2023. Additionally, NTSC made the cyber workforce a core piece of all congressional meetings in 2023. In the wake of the release of the ONCD strategy and NTSC's considerable advocacy in 2023, NTSC feels the cyber workforce issue has been raised to all the right targets. As such, we are removing it as a top five policy priority. However, developing the cyber workforce remains a crucial part of our collective defense, and NTSC will continue to monitor ONCD's implementation of its strategy.

Critical Infrastructure

The NTSC will continue to emphasize the importance of IT/OT integration. Whether it is the energy sector, water utilities, oil and gas, or transportation infrastructure, OT remains a major concern. In a discussion delivered at *Hack the Capitol* in May 2023, Rear Admiral (Ret.) Mark Montgomery, who leads the Cyberspace Solarium Commission 2.0, criticized the sector-specific critical infrastructure security plans developed by the federal government. He said that the Department of Homeland Security "wrote one sector plan in 2015, probably for the chemical sector," and other agencies "word searched the name of their sector and then replaced them" when making their own plans.

Continuing to Strengthen the Public-Private Partnership

The NTSC continues to work with CISA and our congressional leaders to ensure they are hearing the voice of the CISO. Only through collaboration between the public and private sector can we ensure our collective defense. As CISA Director Jen Easterly and Assistant Director for Cybersecurity Eric Goldstein said in a February 2023 article in *Foreign Affairs*, the government must "move to a posture of persistent collaboration. Such a culture shift requires that sharing become the default response, where information about malicious activity, including intrusions, is presumed necessary for the common good and urgently shared between industry and government."

COALITION GROWTH

2023 was a phenomenal year for growth with 12 new members joining the NTSC Board along with several new members also joining the NTSC Policy Council.

However, we experienced a slightly higher level of churn with 7 board members stepping down from the board for a variety of reasons, including budget constraints, bandwidth issues, and in one case the executive moved from a CISO role to becoming the CEO of a firm

From a personal perspective, I am delighted that Murray Kenyon (U.S. Bank) has accepted the leadership role for the board development committee as we strive to grow the board to a total of 70 members

We finished this past year with 57 board members and a small pipeline leading into the new year, but that pipeline needs to grow significantly and with your support we can make that happen.

We are asking once again for our current board members to look into your personal network and recommend one CISO to our board development committee. We need to grow in the retail, manufacturing, energy, transportation and entertainment sectors and welcome your support. We will provide the requisite introduction collateral so that you can position the coalition in the best possible light, leaving the recruitment process to our board development committee, but we need you to identify the candidates and provide the initial introduction.

From an inaugural board of 7 members in 2016 to a coalition of 82 senior technology security executives including Chief Information Security Officers, Chief Risk Officers, Chief Trust Officers, Chief Privacy Officers, Chief Information Officers, Governmental Affairs Executives and a Leading Cyber Attorney, the NTSC has continued to mature and today represents a serious voice on Capitol Hill.

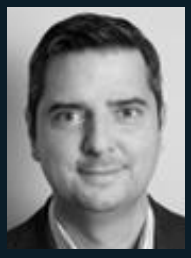
We look forward to another year of growth, both in terms of the coalition membership as well as our influence in Washington, D.C.

NEW BOARD MEMBERS 2023

Katherine Kuehn
CISO in transition

Dr. Adrian Mayers
Premera Blue Cross

David Lin
The Gemological Institute of America, Inc.



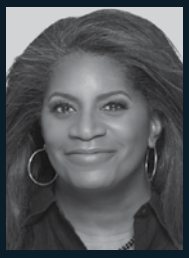
John Dunn
Accuray

Saša Zdjelar
ReversingLabs

Mario Balakgie
World Wide Technology, Inc.

Forrest Smith
Ingram Micro

Billy Spears
Teredata



Beth-Anne Bygum
Q2, Inc.

Benjamin Murphy
Unum Group

James Eckart
Microsoft Corporation

Jacob Lorz
Cintas

2023 BOARD OF **DIRECTORS**

OFFICERS

- **Tim Callahan**—Aflac (Chair)
- **Jason Witty**—USAA (Vice Chair)
- **Larry Williams**—TAG (President)
- **Michael Blache**—TaxSlayer (Treasurer)
- **Kristin Cornish**—Coca Cola (Secretary)

BOARD MEMBERS

- **Marene Allison**—Special Advisor
- **Geoff Aranoff**—GE Healthcare
- **Ben Aung**—The Sage Group
- **Mario Balakgie**—World Wide Technology
- **Martin Bally**—Campbell's Soup Company
- **Scott Benson**—Edward Jones Investments
- **Don Boian**—Hound Labs
- **Beth-Anne Bygum**—Q2 Solutions
- **Janet Cinfio**—Acxiom
- **Jason DeVoe**—Voya Financial
- **John Dickson**—Colonial Pipeline
- **Jim Eckart**—Microsoft Corporation
- **Joe Ellis**—Ryder Systems, Inc.
- **Paul Farley**—NCR Boyix Coporation
- **Jamil Farshchi**—Equifax
- **Kevin Gowen**—Synovus
- **Ron Green**—Mastercard Corporation
- **Stacey Halota**—Graham Holdings
- **Gary Harbison**—Johnson & Johnson
- **Shawn Harris**—Chipotle Mexican Grill
- **Lori Havlovitz**—Haleon
- **Curley Henry**—Southern Company
- **Darren Highfill**—Norfolk Southern Corporation
- **Wayne Hilt**—Huntington National Bank
- **Stacy Hughes**—ABM Industries
- **Shaun Khalfan**—Discover Financial Services
- **Donna Kidwell**—Arizona State University
- **Murray Kenyon**—U.S. Bank
- **Kate Kuehn**—CISO in Residence
- **David Lin**—Geomological Institute of America
- **Jacob Lorz**—Cintas
- **Dr. Adrian Mayers**—Premera Blue Cross
- **Kevin McKenzie**—CISO in Residence
- **Michael McNeil**—McKesson
- **Lucia Milică**—Stanley Black & Decker
- **Allison Miller**—UnitedHealth 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
- **Eric Seagren**—Oceaneering
- **Forrest Smith**—Ingram Micro
- **Mark Strosahl**—Penn Mutual
- **Billy Spears**—Teradata
- **Brian Waeltz**—Cardinal Health
- **Steven Weber**—AbbVie
- **Howard Whyte**—Truist Financial
- **Reginald Williams**—The Chemours Company
- **Saša Zdjelar**—ReversingLabs

9,856,348

Cyber attacks prevented today.

Just another day of Security In Action.

checkpoint.com/action

CHECK POINT™

Estimate based on average calculation from ThreatCloud AI January 2024, an AI-powered threat intelligence engine that makes over 2 billion security decisions daily allowing us to provide accurate prevention in under 2 seconds to hundreds of millions of enforcement points worldwide. We'd say more but...you get the point.

30 YEARS OF THE BEST SECURITY

PROGRAMMING

2023 Events

In 2023 we hosted regional policy roundtables in Washington, D.C. in March, New York City in May, and Atlanta in September. We also hosted our National CISO Policy Conference in Washington, D.C. in July. Unfortunately, we had to move our St. Louis regional event, which was scheduled for November of last year to January of 2024 due to an unusually low number of registered guests, which has resulted in our scheduling all of our 2024 regional events in the first nine months of the year. We have learned that travel budgets are typically curtailed in Q4 for most companies, so in 2024 we will focus on virtual events in the fourth quarter.

In 2023 we focused on five policy priorities:

- Harmonizing Cyber Incident Reporting
- Establishing a Federal Privacy Mandate
- Establishing a Holistic National Cyber Workforce Strategy
- Establishing a National Strategy to Protect Critical Infrastructure
- 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 artificial intelligence, cyber threat intelligence, ransomware, third party risk management, especially software supply chain management, and of course the new cybersecurity regulations adopted by the SEC.

We heard from multiple speakers during the year including:

- Jen Easterly, Director of the Cyber Security & Infrastructure Security Agency (CISA)
- Nick Leiserson, Assistant NCD for Cyber Policy & Programs, Office of the National Cyber Director (ONCD)
- Cory Simpson, Founder & CEO, Gray Space Strategies
- Emilian Papadopoulos, President, Good Harbor Security Risk Management
- Brandon Pugh, President, Policy Director & Resident Senior Fellow for the Cybersecurity & Emerging Threats, R Street Institute
- Kathleen Scott, Partner & Attorney at Law
- Wiley Rein, LLP, moderated by Courtney Stout, Chief Privacy Officer, The Coca Cola Company

Our programming provides our members and select guests with an opportunity to have candid conversations with key players including members of congress.

- Eric Goldstein, Executive Assistant Director for CISA
- Rear Admiral (Ret.) Mark Montgomery, Senior Director of CCTI and Senior Fellow at Foundation for Defense of Democracies (FDD) and Executive Director
- Oki Mek, Federal Civilian Chief Information Security Officer for Microsoft Corporation
- Rhett Krulla, Chief Technology Officer for the Homeland Security Division at Microsoft Corporation
- Elias (Lou) Mansousos, Corporate Vice President, Microsoft Corporation
- Vice Admiral (Ret.) T.J. White, Nonresident Senior Fellow, Forward Defense Practice of the Atlantic Council's Scowcroft Center for Strategy & Security;

Senior executives from our national underwriters included:

- Kelly Bissell, Corporate Vice President at Microsoft
- Mario Balakgie, Global Business CISO at World Wide Technology
- Lucia Milica, Global Business CISO at Proofpoint, Inc.

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 2023 the NTSC, in partnership with Commonwealth Strategic Partners, our full-time representative in D.C., was able to meet with 103 congressional offices throughout the year, sometimes to simply introduce the NTSC, and more often to discuss our policy priorities, especially our efforts to drive towards a national privacy mandate.

Returning to the attendance issues experienced in Q4 of last year, the reality is we are still falling short of our attendance goals at each event with the exception of the national conference and would encourage each of our members to review the event dates for 2024 that we have published in Boardable and ask that you make every effort to lock into at least one regional roundtable and the national conference.

On another note, we did visit the UK again in 2023 to meet with UK based CISOs as well as several government offices, but strictly on a exploratory basis as any effort to extend our presence in the UK will be postponed until at least 2025 to give us ample time to expand our presence domestically, which was highlighted in the study conducted by PwC last summer.

PARTNERING

Today, cyber threats loom large, and the digital landscape continues to evolve rapidly, which makes the collaboration between public and private entities a critical 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.

Public-private partnerships provide a multifaceted approach to cybersecurity, leveraging the strengths of both sectors. Private enterprises bring agility, innovation, and specialized expertise to the table, while governmental bodies offer regulatory frameworks, intelligence, and enforcement capabilities. By pooling resources and sharing information, these partnerships create a synergistic ecosystem capable of identifying and mitigating cyber threats more effectively.

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 the Cybersecurity & Infrastructure Security Agency (CISA), a relationship we have fostered since our earliest days. We have also developed a solid working relationship with the Office of the National Cyber Director (ONCD) and ancillary organizations like the Foundation for the Defense of Democracies (FDD), the Aspen Cyber Institute, the Bipartisan Policy, Gray Space Technologies and the R Street Institute. 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.

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).

Furthermore, public/private partnerships enable coordinated incident response and recovery efforts in the wake of cyberattacks. By establishing communication channels and protocols beforehand, public and private entities can swiftly coordinate their response efforts, minimize damage, and restore normal operations. This collaborative approach not only reduces the impact of cyber incidents but also enhances the resilience of the overall cybersecurity ecosystem.

Beyond the obvious operational benefits, public/private partnerships play a pivotal role in shaping the political landscape surrounding cybersecurity. In an increasingly interconnected world, cyber threats transcend national borders, necessitating international cooperation and coordination. Public-private partnerships serve as a bridge between governments, fostering diplomatic relations and promoting trust and transparency in cyberspace.

Moreover, these partnerships help address the inherent tension between security and privacy concerns. By engaging in dialogue and collaboration, stakeholders can strike a balance between protecting sensitive information and ensuring individual liberties. This collaborative approach enhances public trust in both governmental and private institutions, thereby strengthening the legitimacy of cybersecurity initiatives and policies.

The NTSC recognizes the importance of public-private partnerships in cybersecurity. From an operational perspective, these collaborations enhance threat detection, incident response, and resilience. Politically, they foster international cooperation, address privacy concerns, and bolster public trust. As cyber threats continue to evolve in sophistication and scale, leveraging the collective resources and expertise of both sectors is essential in safeguarding our digital infrastructure and promoting a secure and resilient cyberspace.

LEGISLATIVE AND AVOCACY UPDATE

Despite a chaotic year in Congress as the House struggled to elect and maintain a Speaker and both chambers wrestled with slim majorities, NTSC and Commonwealth Strategic Partners had a very productive year. CSP and NTSC conducted over 100 meetings with members of Congress and their staff, doubling the number held in 2022. CSP also spearheaded several key events, projects, and initiatives on behalf of NTSC, including securing legislators to speak at the Annual National CISO Policy Conference and coordinating a staff briefing hosted by NTSC for staffers of members of Congress who serve on the House Energy and Commerce Committee.

Additionally, each month, CSP provided NTSC with a detailed report on relevant legislative and regulatory developments. CSP attended monthly Strategic Direction Committee meetings and quarterly Board and Police Council meetings.

The CISA Cybersecurity Advisory Committee (CSAC), whose creation was spearheaded by NTSC and CSP, held quarterly meetings throughout 2023. CSAC membership includes NTSC board members Ron Green of Mastercard and Marene Allison, formerly of Johnson & Johnson. Mr. Green serves as Vice Chair and Ms. Allison serves on the subcommittee on Building Resilience and Reducing Systemic Risk to Critical Infrastructure.

The chaotic leadership and legislative battles in Congress did not deter NTSC and CSP from our mission to advocate for CISOs. With the retirement of longtime allies Representatives John Katko and Jim Langevin, CSP worked to identify and meet with new cybersecurity policy leaders. Meetings early in 2023 included new House Cybersecurity Subcommittee Chair Representatives Andrew Garbarino (R-NY) and new house Cybersecurity Subcommittee Ranking Member Eric Swalwell (D-CA).

Finally, congressional chaos did not impede major cybersecurity policy developments, some of the most important of which are detailed below.

In March, the Biden Administration released its long-awaited National Cybersecurity Strategy. The strategy opens with a letter from President Biden detailing the integral function cybersecurity takes in securing our economy, critical infrastructure, and national defense. Drawing on the evolutionary nature of our nation's cyberspace, the strategy outlines five pillars to cyber resilience: (1) defend critical infrastructure, (2) disrupt and dismantle threat actors, (3) shape market forces to drive security and resilience, (4) invest in a resilient future, and (5) forge international partnerships to pursue shared goals. The strategy encompasses two fundamental shifts in how the U.S. allocates cyber resources, talent, and responsibility. The first shift reallocates cyber mitigation responsibility from smaller actors–small businesses, individuals, state and local governments, and infrastructure operators–towards larger entities better suited to secure our cyber space. The second shift involves prioritizing long-term investments by establishing a strong cyber workforce, investing in research and development, and promoting collaboration.

In May, the White House released new guidance: National Standards Strategy for Critical and Emerging Technology. The strategy focuses on four foundational priorities for developing critical and emerging technologies standards: investment, participation, workforce, and integrity & inclusivity, as explained in a White House fact sheet. NIST will serve as the lead agency in implementing this strategy. Additionally, the agency released their own fact sheet detailing their roles and responsibilities throughout the implementation process.

Additionally, in May, President Biden nominated U.S. Air Force Lt. Gen. Timothy Haugh to serve as the head of U.S. Cyber Command and the National Security Agency (NSA). Haugh has a long history of working in cyber including previously leading Air Force Cyber and serving as director of the Cyber Command's Cyber National Mission Force. If confirmed by the Senate, Haugh will replace Gen. Paul Nakasone who has led both the NSA and Cyber Command since 2018.

July was a particularly busy month for cybersecurity policy.

Firstly, President Biden nominated Harry Coker, Jr., to serve as National Cyber Director. Coker has served for more than forty years in public service, including leadership roles in the U.S. Navy, CIA, and NSA. The nomination followed Acting Director Kemba Walden's announcement she is withdrawing her nomination for the position due to concerns about her personal debts.

Secondly, the SEC approved a cybersecurity regulation ordering incident reporting and cyber risk management requirements for all publicly traded companies. The rule was approved in a 3-2 vote, with the SEC split along partisan lines. The rule requires publicly traded companies disclose material cyber incidents within four days of the time the company determines a material event has occurred. The ruling will become effective thirty days after publication in the Federal Register. The SEC released a fact sheet on the rule.

Finally, the Office of the National Cyber Director released the National Cyber Workforce and Education Strategy. This strategy outline four pillars to enhance collaboration on workforce development and address to current shortage of cyber workers: (1) Equip Every American Foundation with Foundational Cyber Skills; (2) Transform Cyber Education; (3) Expand and Enhance America's Cyber Workforce; and (4) Strengthen the Federal Cyber Workforce. The ONCD is tasked with leading the implementation of the strategy.

In August, CISA published an FY2024-2026 Cybersecurity Strategic Plan. The Strategic Plan outlines three goals and explores CISA's plans for achieving them: (1) Address Immediate Threats, (2) Harden the Terrain, and (3) Drive Security at Scale. The plan aligns with the Biden Administration's National Cyber Strategy. You can read CISA's blog post on the publication here.

In September, the Senate confirmed Anna Gomez for a seat on the FCC, giving the FCC a 3-2 Democrat majority. Following that, FCC Chair Jessica Rosenworcel announced FCC's intentions to restore net neutrality regulations while signaling that national security will be a top priority.

In December, the Senate voted to confirm Harry Coker as National Cyber Director. Prior to the confirmation vote, Senate Homeland Security Chair Gary Peters (D-MI) spoke on the floor on Coker's behalf, saying, "Harry Coker is an accomplished leader and a dedicated public servant who is well qualified to lead this important office." Coker previously worked for NSA and the CIA.

Additionally, in December, the Senate voted to confirm U.S. Air Force Lt. Gen. Timothy Haugh to serve as the head of U.S. Cyber Command and the National Security Agency (NSA). Haugh has a long history of working in cyber including previously leading Air Force Cyber and serving as director of the Cyber Command's Cyber National Mission Force.

In 2024, NTSC will focus its advocacy efforts on advocating for a federal privacy mandate while monitoring developments in incident reporting harmonization and cyber workforce development. NTSC will also work to foster relationships with established cyber leaders on the Hill while constantly seeking new allies among those members of Congress eager to establish themselves in the cyber policy space. Given the narrow margins in both chambers of Congress, NTSC and CSP believe that our bipartisan focus will remain a winning strategy.

NAVIGATING THE HORIZION:
THE FUTURE OF CYBERSECURITY IN 2024

As we move into 2024, the landscape of cybersecurity is poised for both unprecedented challenges and groundbreaking advancements.

As we move into 2024, the landscape of cybersecurity is poised for both unprecedented challenges and groundbreaking advancements. At the forefront of this evolution are the interplay of artificial intelligence (AI), the dynamic global threat landscape, the potential for innovative cyber legislation amidst an election year, and the profound geopolitical factors shaping cyber decisions.

Artificial intelligence stands as a double-edged sword in the realm of cybersecurity. On one hand, AI has emerged as a formidable ally in the battle against cyber threats, offering predictive analytics, threat detection, and autonomous response capabilities. However, the proliferation of AI-driven cyberattacks poses a significant concern. Malicious actors leverage AI to craft sophisticated attacks, evade detection, and exploit vulnerabilities at an unprecedented scale. As AI continues to mature, cybersecurity professionals must harness its power while fortifying defenses against AI-enabled threats.

At the same time, Congress is grappling with the need to create guardrails that protect our children and our privacy, but do not hamper innovation and

The reality is, 2024 is going to be a challenging year and staying in front of our congressional leaders will be a priority and will require the support of all of our members.

the need to stay ahead of China, which has which has 11% of top-tier AI researchers (Macro Polo) and has raised $95 billion in private investment between 2022 and 2023, according to Mirae Assets. Today, while the US is the most prolific country in AI research, with almost 60% of "top tier" AI researchers working for American universities and companies and $249 billion in private funding having been raised to date, the concept of "pausing" research & development has created significant debate within the scientific community. The NTSC strongly encourages our congressional leaders to create legislation that supports an ethics approach to AI that establishes clear policies and drives accountability throughout the AI lifecycle, but we do not endorse the need for a pause given the competitive threat that China and other hostile nation states pose. The global threat landscape is continuously evolving, characterized by increasingly sophisticated cyber threats spanning nation-state actors, cybercriminal syndicates, and lone-wolf hackers. State-sponsored cyberattacks, in particular, escalate tensions on the geopolitical stage, fueling concerns of cyber warfare and espionage. Recent congressional hearings exploring the existential threat posed by malicious code planted by Chinese hackers, most likely working for the People's Liberation Army (PLA), into U.S. critical infrastructure including power grids, communications systems and water supplies that feed military bases in the United States and around the world demonstrate the challenges the nation faces going forward. Furthermore, the proliferation of Internet of Things (IoT) devices expands the attack surface, amplifying the magnitude and complexity of cyber threats. To mitigate these risks, collaboration and information-sharing between governments, private sector entities, and international organizations will be imperative in 2024 and beyond.

In the midst of an election year, the prospect of innovative cyber legislation looms large. Governments worldwide face mounting pressure to enact robust cybersecurity measures to safeguard critical infrastructure, protect sensitive data, and preserve democratic processes. However, achieving consensus on cybersecurity policies amidst the backdrop of political polarization and partisan interests presents a formidable challenge. The enactment of effective cyber legislation hinges not only on legislative prowess but also on public awareness, stakeholder engagement, and technological expertise. For the past eight years the NTSC has focused on educating our congressional leaders on the challenges faced by security professionals as they deal with multiple threats ranging from well organized criminal elements to nation states, emphasizing the need for legislation that recognizes these challenges. Our mission has always been to bring the cyber practitioner's voice to Capitol Hill and in 2024 we will continue to push for our legislative priorities including the establishment of a federal privacy mandate and the need software supply chain security.

Cybersecurity in 2024 is fraught with both promise and peril. The convergence of artificial intelligence, the dynamic global threat landscape, the potential for innovative cyber legislation in an election year, and the influence of geopolitical factors underscore the complexity of the cybersecurity landscape.

The reality is, 2024 is going to be a challenging year and staying in front of our congressional leaders will be a priority and will require the support of all of our members.

2023 Year In Review

Secure, innovative solutions to guide the modern CISO.

Navigate organizational change with an agile, security-focused delivery partner. Improve your identity management, secure your enterprise data, and prepare your organization for Generative AI.

collective insights
CONSULTING

Ready to raise the bar?

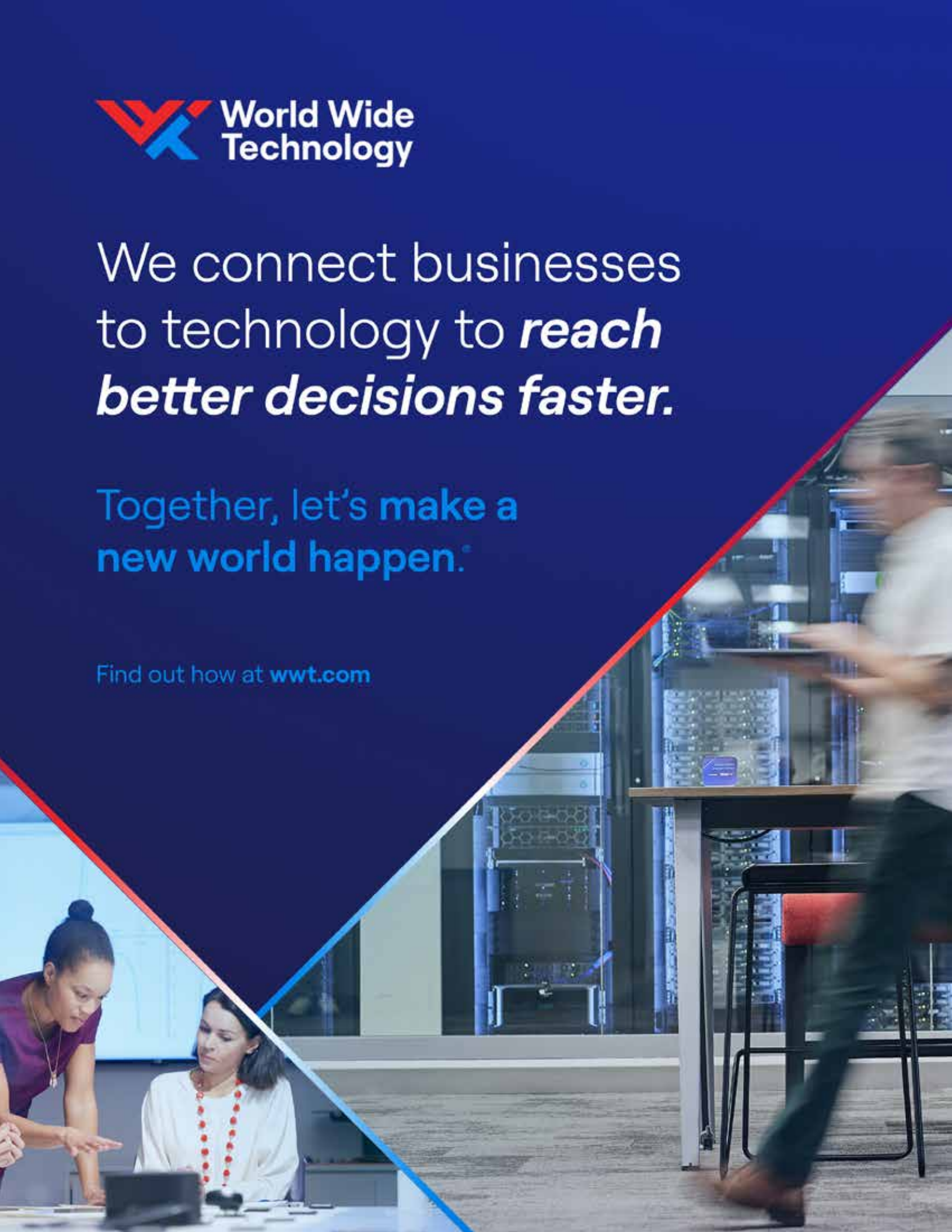
info@collectiveinsights.com
collectiveinsights.com

World Wide Technology

We connect businesses to technology to ***reach better decisions faster.***

Together, let's **make a new world happen.**

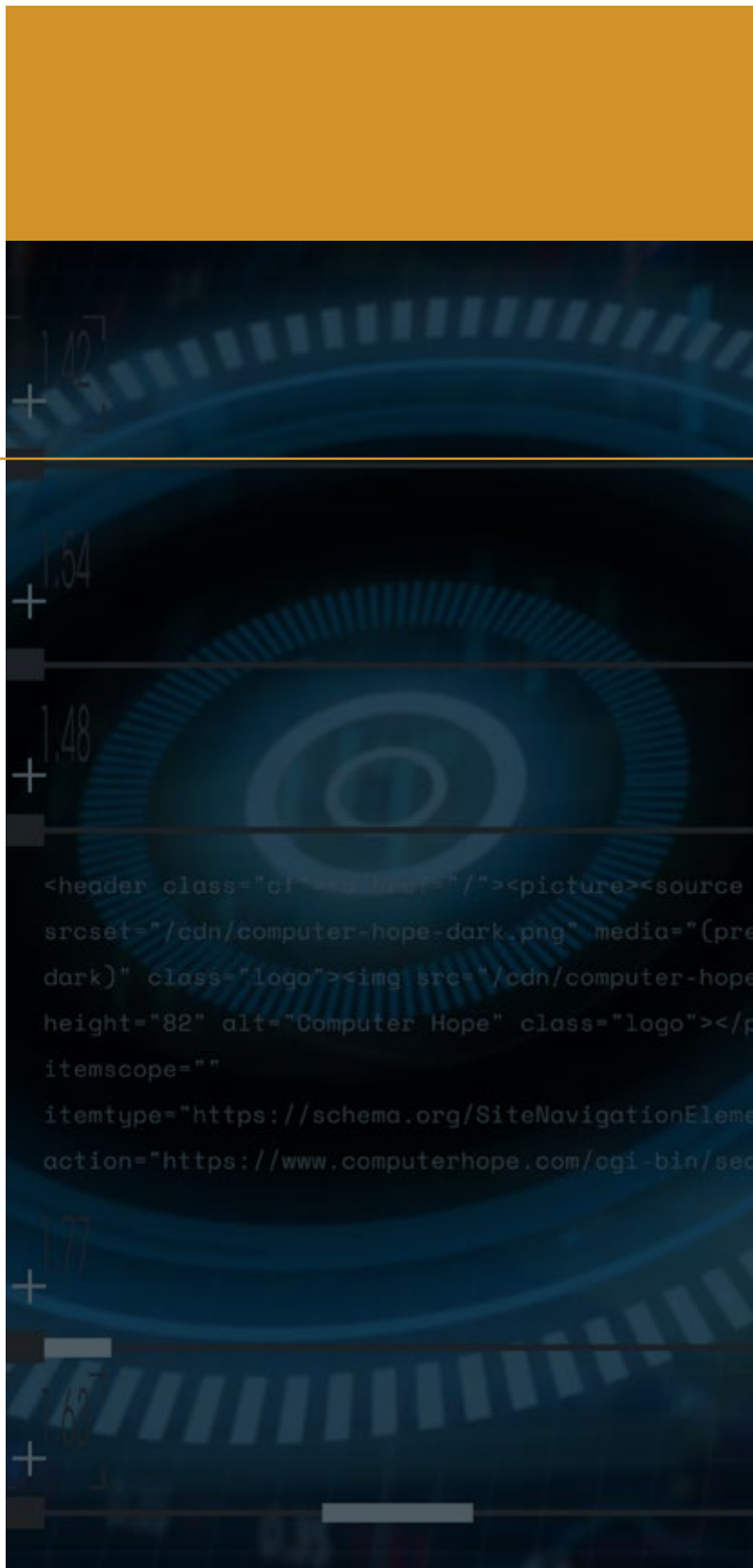
Find out how at **wwt.com**



Larry Williams
President, NTSC
LWilliams@tagonline.org
470.823.3546

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

National Technology Security Coalition
info@ntsc.org



NTSC
NATIONAL TECHNOLOGY
SECURITY COALITION

ntsc.org