NTSC

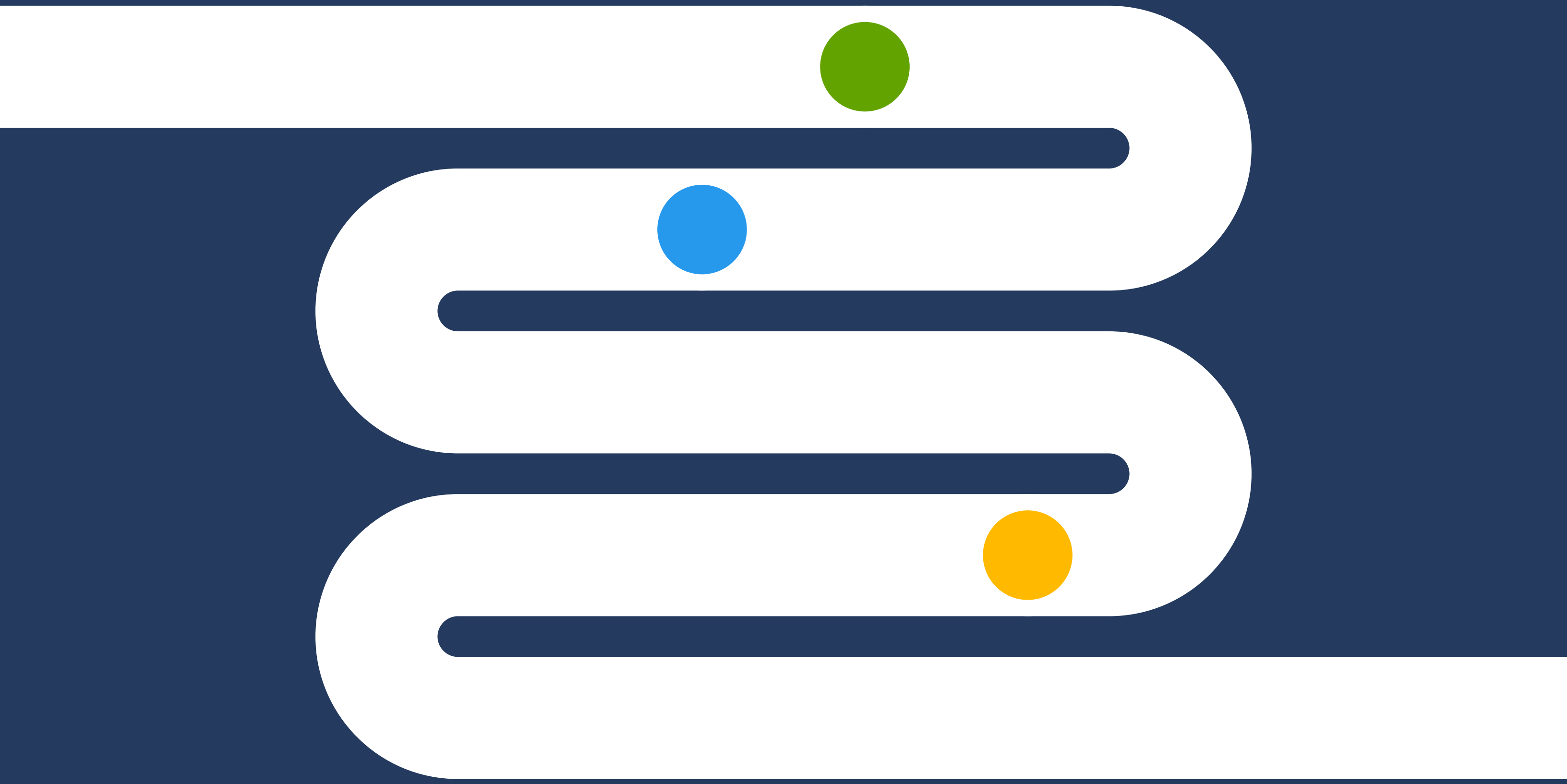
NATIONAL TECHNOLOGY SECURITY COALITION

2022 YEAR IN REVIEW

Microsoft

You have a vision.
We can help you secure it.
Be fearless.

Learn more at www.microsoft.com



NTSC
NATIONAL TECHNOLOGY
SECURITY COALITION

MISSION STATEMENT

The National Technology Security Coalition (NTSC) is a non-profit, non-partisan trade association that serves as the preeminent advocacy voice for the CISO. Through dialogue, education, and government relations, we unite both public and private sector stakeholders around policies that improve national cybersecurity standards and awareness.

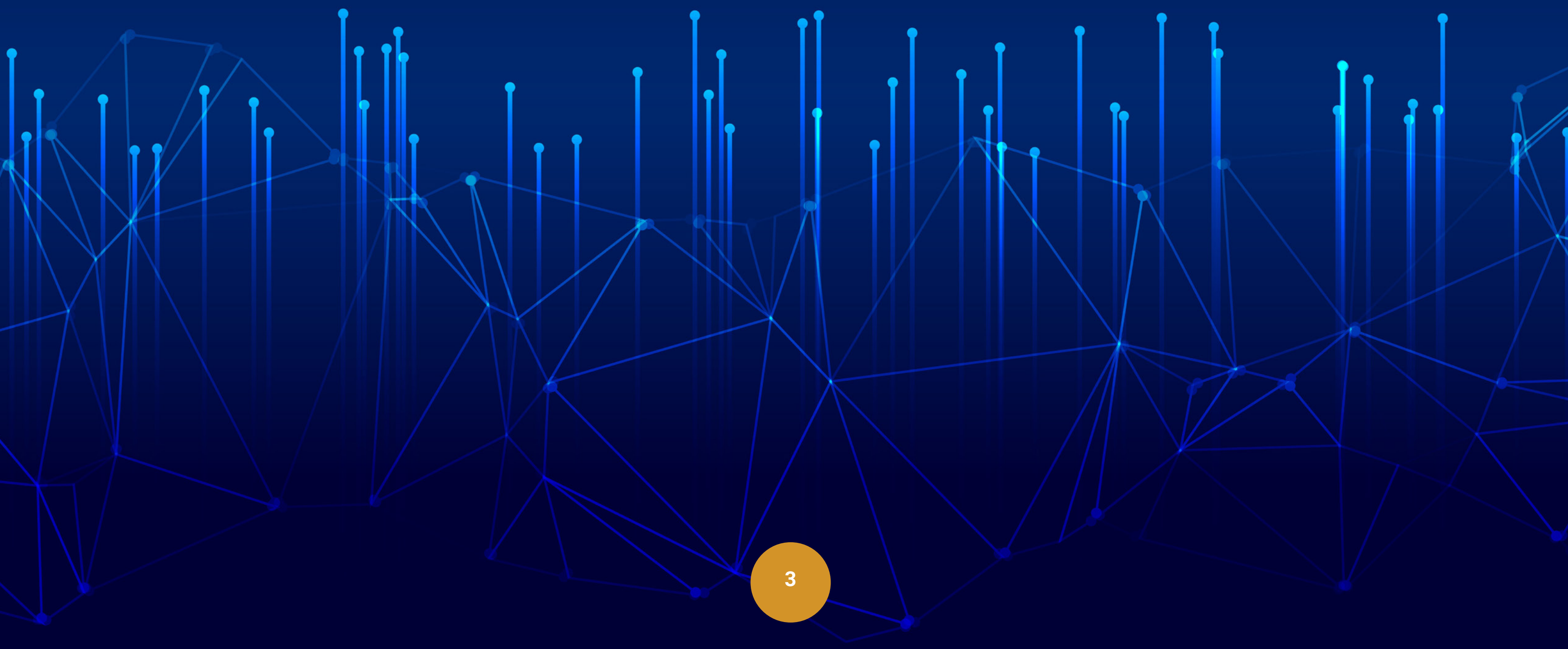


TABLE OF **CONTENTS**

LETTER FROM THE **PRESIDENT**

As the President of the NTSC, I am pleased to present our annual report for 2022. This past year has been a pivotal one for our organization, marked by new additions to our board, changes in leadership and a focus on expanding our reach and impact.

At the NTSC, we are committed to being the pre-eminent voice of the private sector CISOs. Our main goal is to advance policies and partnerships in order to address global cybersecurity privacy and the growing demand for a skilled workforce. These topics are more important today than ever, which makes our work all the more critical. The issues we address extend beyond the borders of the United States. As such we are pleased to have hosted our first international CISO round-table in London, England this year.

Our success is contingent on the people who lead the NTSC. I want to thank the NTSC Board of Directors for their hard work and especially Tim Callahan, CISO for Aflac, for his continued leadership and passion to improve cybersecurity policy and awareness. Also, I am thrilled to announce that we have welcomed ten new members to our board, including Allison Miller, CISO for Optum, Mark Strosahl, CISO for Penn Mutual and Mick Coady of Worldwide Technology. Additionally, we saw a number of changes within our board as members transitioned into new roles. Lori Havlovitz moved from Cardinal Health to GSK Consumer Health, which later evolved to become Haleon, and Marene Allison, who, after retiring from her position as the Global CISO at Johnson & Johnson, has accepted our invitation to serve as a Special Advisor to the NTSC Board of Directors.

This year, our partnership with Commonwealth Strategic Partners (CSP) has been instrumental in aiding our advocacy efforts. In addition to countless phone calls and email exchanges, CSP conducted more than 50 formal meetings with congressional and committee staff, federal regulators and relevant third-party organizations such as the Cyberspace Solarium Commission. CSP also spearheaded several key events, projects and initiatives on behalf of NTSC, and provided us with a detailed report on relevant legislative and regulatory developments each month. And, our combined efforts led to the creation of the CISA Cybersecurity Advisory Committee (CSAC), which held quarterly meetings throughout the year. We will continue to work closely with CSP and other partners to advance the interests of CISOs and the cybersecurity industry as a whole.

In terms of events, we hosted regional policy roundtables in Atlanta in February, New York City in May, Chicago in September, London in October and Seattle in November. We also hosted our national conference in Washington, D.C. in July. The feedback we received from these events suggests that we need to broaden our focus beyond the five policy priorities established at the beginning of the year, and diversify our guest speakers so that we can hear from experts across a wide range of disciplines. In conclusion, while there were many developments in 2022, we still have much work to do in order to reach our goals and continue to provide valuable resources and support to our members.

As we move forward into 2023, we remain committed to being a leading voice in the technology security industry. We have an incredible Executive Director, Patrick Gaul, who works tirelessly to advance the NTSC. I look forward to working with our dedicated team and board of directors to achieve our objectives in the coming year.

Sincerely,

Larry Williams
President
National Technology
Security Coalition

POLICY UPDATE

Harmonizing Cyber Incident Reporting Requirement

The NTSC believes it is essential that we have one standard for cyber incident reporting, preferably following the guidelines articulated in the CISA Incident Reporting Act passed by Congress last year. However, with other federal agencies including the SEC, the FTC, and now the FCC all looking at passing legislation that includes incident reporting, it will be important that we continue to advocate for a single standard.

Continuing to advocate for a Federal Privacy Mandate

In January 2023 eleven states (Oregon, Nevada, Indiana, Oklahoma, Mississippi, Tennessee, Kentucky, Iowa, New York, Massachusetts, and New Jersey) introduced privacy legislation. California and Virginia privacy laws took effect on January 1. Colorado and Connecticut privacy laws will be effective on July 1 and Utah's Consumer Privacy Act will become effective on December 31, 2023. It is clear that we are headed down the same path as Data Breach Notification and unless Congress acts swiftly the states continue to enact legislation, which will make preemption significantly more challenging.

Establishing a holistic, national strategy focused on resolving the cyber workforce challenges

While there are many efforts to address this national concern including the Microsoft Community College Campaign, the reality is they are not coordinated and without a holistic national strategy we will continue to struggle to meet the challenges created by the cyber workforce shortages. We have to move beyond the headlines and focus on the real issues including the lack of diversity. Expanding the CyberCorps for Service Program is one approach, but that will require additional funding and expanding the number of colleges and universities currently associated with the program, which will be a challenge in the 118th Congress and as previous experience has shown, legislation does not happen fast on Capitol Hill.

Critical Infrastructure

The NTSC will continue to emphasize the importance of IT/OT integration, often driven by digital transformation initiatives. Whether it is the energy sector, the water utilities, oil and gas, or transportation infrastructure, Operational Technology (OT) continues to be a major concern. As Alex Bagwell, Vice President at Tripwire noted in an article published in August of 2021 (What Are the Key Challenges Facing IT and OT? | Tripwire), "the biggest challenges that we are seeing with IT-OT convergence is how to consolidate overlapping solutions across multiple business units within seemingly separate IT and OT networks.

Continuing to strengthen the public/private partnership

As Kiersten Todt, the Chief of Staff at the Cybersecurity & Infrastructure Agency (CISA) noted in her forward to "Fixing American Cybersecurity", "neither the private nor the public sector can effectively address cybersecurity on its own. Effective collaboration between the government and industry is an absolute must for improving this nation's cybersecurity posture." The NTSC continues to work with our congressional leaders to ensure they are hearing the Voice of the CISO, the practitioner in this national issue through individual meetings with congressional leaders, our annual legislative day, and working with other stakeholders including CISA.

COALITION GROWTH

While there was good movement in terms of adding new members and keeping members who transitioned into new roles, we only experienced a net growth of five new members in 2022, falling far short of our goal of sixty by 12.31.22, which provides us with a challenge in 2023 as we continue to expand the board. We may be able to supplement our U.S. board presence with additional members in the UK and that will certainly be a focus for us in 2023 as we plan out our second international roundtable in London on September 28, 2023, but it is also important that we continue to grow our domestic presence given our experiences last year.

The reality is CISOs transition into new roles and they are not always able to persuade the new firm to sponsor their memberships, or as is more frequently the case, the transitioning CISO doesn't have the bandwidth to continue to serve after taking on a new role. So, for every new member we add we have to recognize that we will lose members during the year, and we will also need to compensate for the losses we know will occur. This means that to get to sixty from where we are today (fifty), we will need to add at least fifteen new members in 2023 based on previous years.

New Board Members 2022

Allison Miller
CISO for Optum

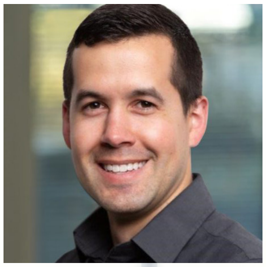
Lucia Milica
Vice President & Global Resident CISO for Proofpoint, Inc.

Shawn Harris
Director, Information Security & ISO for the America's for Starbucks

Curley Henry
Executive Director, Cybersecurity Strategy and Architecture for The Southern Company

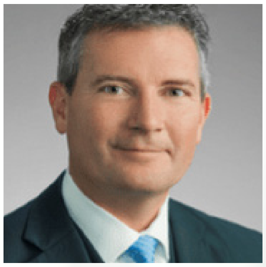
Reginald Williams
CISO for The Chemours Company

Martin Bally
CISO for the Campbell Soup Company



Mark Strosahl
CISO for Penn Mutual

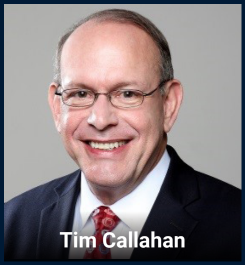
Howard Whyte
CISO for Truist



Mick Coady
Worldwide Technology

COALITION GROWTH (cont.)

NTSC Board Members

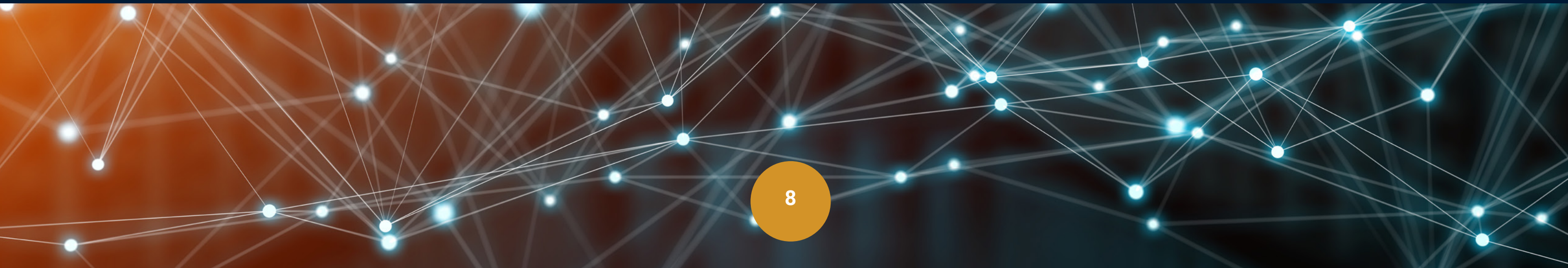

Tim Callahan

Officers

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

Board Members

- **Marene Allison**—Special Advisor
- **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
- **Matt Cairns**—Eli Lilly & Company
- **John Dickson**—Republic National Distributing Company
- **Jim Eckart**—Microsoft Corporation
- **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
- **Timothy Held**—U.S. Bank
- **Curley Henry**—Southern Company
- **Darren Highfill**—Norfolk Southern Corporation
- **Wayne Hilt**—Huntington National Bank
- **Stacy Hughes**—Voya Financial
- **Shaun Khalfan**—Discover Financial Services
- **Donna Kidwell**—Arizona State University
- **Kate Kuehn**—AON
- **Phil Malatras**—Western Digital Corporation
- **Dr. Adrian Mayers**—Premera Blue Cross
- **Kevin McKenzie**—CISO in Residence
- **Michael McNeil**—McKesson
- **Lucia Milică**—Proofpoint, Inc.
- **Allison Miller**—UnitedHealth Group/Optum
- **Mat Newfield**—Unisys
- **David Nolan**—Aaron's
- **Michael Palmer**—Hearst
- **Mike Priest**—Globe Life
- **Steve Pugh**— InterContinental Exchange
- **Stephen Richardson**—Scientific Games
- **Ray Rothrock**—RedSeal, Inc.
- **Richard Rushing**—Motorola Mobility
- **Eric Seagren**—Oceaneering
- **William Shields**—TransUnion
- **Mark Strosahl**—Penn Mutual
- **Bob Varnadoe**—NCR
- **Brian Waeltz**—Cardinal Health
- **Steven Weber**—AbbVie
- **Howard Whyte**—Truist Financial
- **Reginald Williams**—The Chemours Company



PROGRAMMING

2022 Events

In 2022 we hosted regional policy roundtables in Atlanta in February, New York City in May, Chicago in September, London in October, and Seattle in November. We also hosted our national conference in Washington, D.C. in July of 2022.

The feedback we received from the regional events suggests we need to broaden our focus beyond the five policy priorities we established at the beginning of 2022. Some of the topics suggested included:

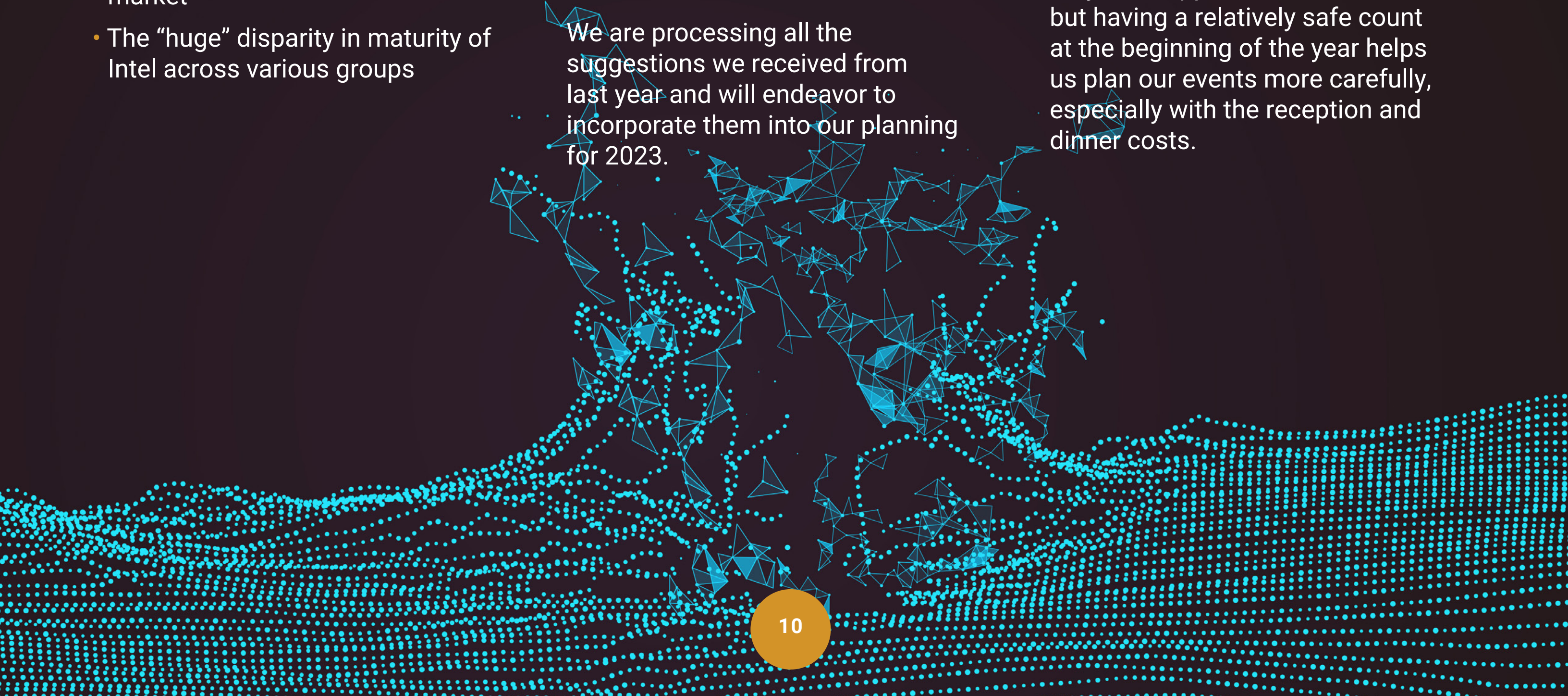
- Third Party Risk Management
- Threat Intelligence
- Identity & Access Management
- Resilience
- Market Consolidation within the vendor community
- The need for an "ISAC" 2.0
- The challenges of small businesses versus the enterprise market
- The "huge" disparity in maturity of Intel across various groups

We also heard that we needed to diversify our guest speaker selection so that we can hear from experts across a wide range of disciplines.

Several members pointed to the national conference and were impressed with the speakers we hosted including the Chris Inglis, the National Cyber Director, Congressman John Katko, the then ranking member on the House Committee for Homeland Security, Sue Gordon, the former Principal Deputy Director of the National Intelligence Agency, and Rear Admiral (Ret.) Mark Montgomery, the former Executive Director of the Cyberspace Solarium Commission. We also heard from Kelly Bissell, Corporate VP & Global Lead for Security Services at Microsoft Corporation, Lucia Milica, VP & Global Resident CISO at Proofpoint, Inc., Suzanne Kelly, CEO & Publisher at The Cipher Brief, and Tim Callahan, NTSC Chair and SVP & Global CISO at Aflac.

We are processing all the suggestions we received from last year and will endeavor to incorporate them into our planning for 2023.

Finally, we were all shaking our heads as the attendance levels dropped dramatically after the national conference. There are multiple reasons associated with the attendance issue in the second half of the year including companies curtailing corporate travel budgets, the proliferation of in-person events following two years of COVID, competing priorities at work or at home, and other perfectly valid reasons for members to have withdrawn from an event prior to the day it was hosted. But we also had a number of members who had confirmed they would be attending and then would not show up on the day without any notice, which makes it difficult for a multiplicity of reasons. Our goal for 2023 is for members to only commit to those events they are relatively certain they can attend, keeping in mind that every board member commits to attending at least one regional event per year. We recognize that things may still happen at the last minute but having a relatively safe count at the beginning of the year helps us plan our events more carefully, especially with the reception and dinner costs.



PROGRAMMING (cont.)

Summary

While our primary focus will always be on what is happening in Washington, D.C. and the various states that capture our attention, especially around privacy legislation, our regional roundtables and national conference are designed to facilitate an exchange of views on the topics that matter most to our community while hearing from subject matter experts from both the public and private sectors.

Over the past several years we have developed a strong relationship with the Cybersecurity & Infrastructure Security Agency (CISA), which supported many of our regional events this year to ensure the dialogue between CISA and the CISO community continues to thrive.

Our National Underwriters, Microsoft Corporation, Proofpoint, Inc., and Worldwide Technology have also significantly contributed to our regional events by providing subject matter experts across a wide range of topics, including privacy, the need for more board level engagement in the understanding the cyber posture of the enterprise, cyber workforce development, and other important issues.

The goal for 2023 is to try to incorporate all of the input we have received during 2022 and make each event we host unique with special guest speakers and focusing on the issues that matter with a continued emphasis on cyber policy and legislation.

Regional Policy Roundtable
New York City | May 2022

Regional Policy Roundtable
London | October 2022

Regional Policy Roundtable
Seattle | November 2022

PARTNERING

A cornerstone of the NTSC is advancing the public/private partnership by bringing the voice of the Chief Information Security Officer (CISO) and other key security stakeholders to the halls of Congress and our federal agencies.

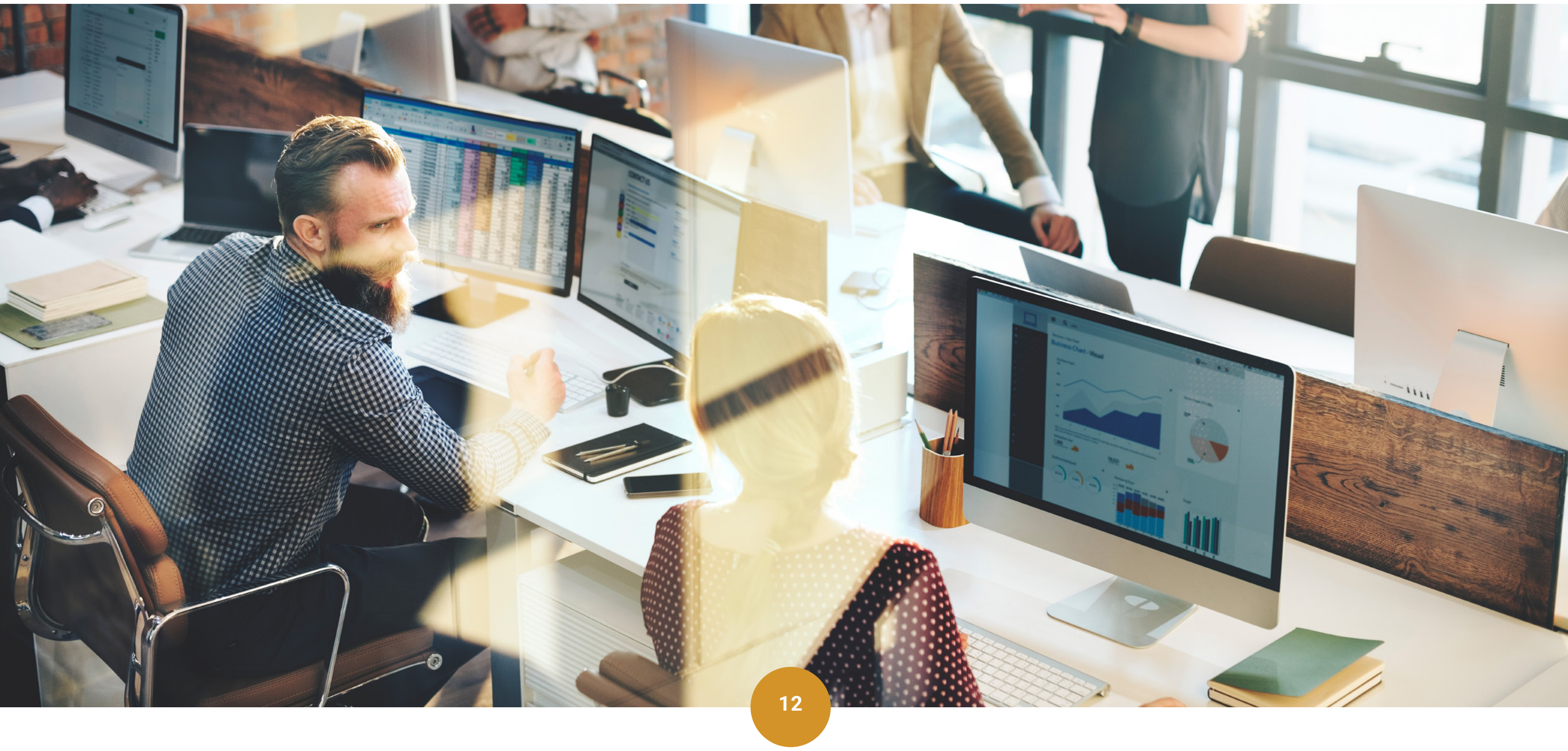
The Federal Government, through the Cybersecurity and Infrastructure Security Agency (CISA), has recognized the importance of public-private partnerships in cybersecurity. As threats to our nation's security increase in sophistication and scope, collaboration between government and private sector entities is essential for developing comprehensive strategies that will protect us all. Through information sharing, best practices identification, and improved coordination efforts, these partnerships can provide a collective defense against cyber-attacks.

CISA works closely with partners in the private sector to ensure that they are up to date with the latest developments in cybersecurity. This includes sharing threat intelligence data across sectors, so companies have access to valuable information that helps them stay one step ahead of malicious actors. Additionally, CISA is able to leverage the expertise offered by private sector partners to create more effective solutions that can be implemented in the public sector, but the partnership requires trust, which creates transparency and leads to collaboration.

The sad reality, however, is that the trust required is often hampered by restrictions on both sides of the equation. Corporate legal teams are reluctant to share too much detail about issues affecting the corporate bottom line and government officials are often unable to share information in a timely manner due to the confidential nature of the intelligence gathered and declassification is a complicated process, exacerbated by the processing delays in issuing security clearances to private sector stakeholders.

However, the federal government and private sector must continue to work together to ensure the collaboration required to protect ourselves from cyber threats. The public/private partnership in cybersecurity is essential for staying ahead of the latest threats, ensuring our data is secure, and keeping us all safe.

The NTSC will continue to foster strong relationships in Washington, D.C.. ensuring the voices of the cyber practitioners we represent are heard.



LEGISLATIVE AND AVOCACY UPDATE

NTSC and Commonwealth Strategic Partners (CSP) had a very productive year in the advocacy space. In addition to countless phone calls and email exchanges, CSP conducted more than 50 formal meetings with congressional and committee staff, federal regulators, and relevant third-party organizations such as the Cyberspace Solarium Commission. CSP also spearheaded several key events, projects, and initiatives on behalf of NTSC. 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 Policy Council meetings. Finally, at least one representative of CSP attended each of NTSC's four Regional CISO Policy Roundtables.

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

The distractions of the primary and midterm elections did not deter NTSC and CSP from their mission to advocate for CISOs. Sadly, longtime NTSC allies Representatives John Katko (R-NY) and Jim Langevin (D-RI) will retire at the end of the current term. However, their retirement presents an opportunity to identify fresh leaders in the cybersecurity policy space.

CSP identified current and potential leaders and held meetings with their staff to gauge their interest and intentions in the 118th Congress. Key meetings were held with Sen. Gary Peters (D-MI), Chairman of the Senate Homeland Security Committee; Rep. Ritche Torres (D-NY), who served as Vice Chair of the of House Homeland Security Committee in the 117th Congress; and Rep. Dan Crenshaw (R-TX). We believe that those offices will be some of our key allies going forward.

In March, NTSC and CSP worked with Rep. Katko to craft a letter to CISA Director Jen Easterly. The letter encouraged Director Easterly to consider including more CISOs to fill the remaining seats on CSAC. Director Easterly penned a response in April in which she assured Rep. Katko that she "will certainly consider qualified CISOs and other cybersecurity professionals as potential future members." She also acknowledged the CISOs who currently serve on CSAC: "As you may know, we are fortunate to have the CISOs of Apple, Johnson & Johnson, Amazon, and Mastercard, the Chief Information Officer for JPMorgan Chase & Co., as well as the former CISO of Facebook on the CSAC."

In April, NTSC published CISO 2.0, a white paper exploring the evolving role of the CISO. CSP provided a comprehensive overview of the changing regulatory and legislative landscape that CISOs face.

LEGISLATIVE AND AVOCACY UPDATE (cont.)

In June, at its 5th Annual National CISO Policy Conference, NTSC hosted conversations with several key officials. CSP secured the attendance of National Cyber Director Chris Inglis, Senate Homeland Security Chairman Gary Peters, and House Homeland Security Ranking Member John Katko, as well as several other members of Congress and congressional staff.

In September, CISA sought input on implementing the Cyber Incident Reporting for Critical Infrastructure Act. The NTSC Policy Council and CSP worked to submit a formal response to the request for information which collated the concerns and priorities of NTSC members into a cohesive document. CISA received and published the response alongside over 100 other responses from organizations such as Microsoft and the U.S. Chamber of Commerce.

Additionally, in September, Mr. Gaul and CSP attended the Cyberspace Solarium Commission's 2.0 (CSC 2.0) Annual Assessment of America's Cyberspace Resiliency. CSC 2.0 co-chairs Sen. Angus King (I-ME) and Rep. Mike Gallagher (R-WI) led a discussion on the implementation, execution, and stalemates of the Cyberspace Solarium Commission's recommendations outlined in the CSC 2022 Annual Report. They fielded several questions during a Q&A, including one from Mr. Gaul.

In October, Rep. Langevin's office contacted CSP directly to request that the NTSC endorse the Cybersecurity Skills Integration Act. The Congressman's office published a press release announcing the bill which included a quote of endorsement from Mr. Gaul.

In December, Mr. Gaul and CSP met in-person with several key congressional offices to prepare for the upcoming 118th Congress. Mr. Gaul and CSP also discussed NTSC legislative strategy for the upcoming session.

In 2023, NTSC's advocacy strategy will focus on the perennial issues of incident reporting and inter-agency harmonization. NTSC will also focus on a nationwide consumer privacy law, better critical infrastructure security, and a holistic national strategy in pursuit of cyber workforce development. We will also work to establish ties with the new chairman of the House Committee on Homeland Security, Rep. Mark Green (R-TN).

NTSC and CSP believe that, as some of our longtime allies retire and Committee leadership changes, we have a unique and exciting opportunity to find new champions. Additionally, given the close margins in both chambers of Congress, we believe lawmaking will focus on bipartisan issues like cybersecurity. NTSC and CSP look forward to a fresh, productive 2023 as we advocate on behalf of our CISOs.

LOOKING **AHEAD**

In 2023, there is a significant need for robust cybersecurity policy. With the rapid advancement of AI and other advanced technologies, the potential for cyber threats is growing exponentially. It is essential that lawmakers take a proactive stance in protecting citizens from these emerging threats.

To this end, Congress should act swiftly to implement cybersecurity policy that is both comprehensive and effective. Cybersecurity policies must be designed to prioritize the safety of citizens while also meeting the needs of both the private and public sectors.

Additionally, Congress needs to ensure legislation is flexible enough to adapt to threats as they evolve over time. Cyber policy should not only address current threats, but also identify potential vulnerabilities. Cyber legislation should also provide adequate protection to the intellectual property of businesses and individuals, as well as ensure data privacy for all Americans.

Furthermore, government agencies must be held accountable for their compliance with cybersecurity policy. Cybersecurity measures should be regularly monitored and updated in order to remain effective against digital adversaries. Cyber threats must be detailed and communicated to the public to ensure trust and transparency. The Cybersecurity & Infrastructure Security Agency (CISA) launched “Shields Up,” a cyber threat advisory that is issued whenever a new threat is detected, to help address this issue.

In 2023 it is anticipated that cyber threats will be even more sophisticated and far-reaching than ever before. Cybersecurity legislation and policies must remain at the forefront of legislative efforts in order to protect citizens from digital danger.

Cybersecurity must be viewed not just as a matter of national security but also as a human right deserving of adequate legal protection. Cybersecurity policy must be designed to prioritize the security and privacy of citizens while allowing for innovation and progress to continue unabated. It is essential that Congress take a proactive stance in protecting citizens from digital threats now, or else we risk further harm to the nation’s economic future.

Cybersecurity must be viewed not just as a matter of national security but also as a human right deserving of adequate legal protection.

Cybersecurity is a shared responsibility, and all stakeholders must work together to create effective policies that protect individuals, businesses, and governments.

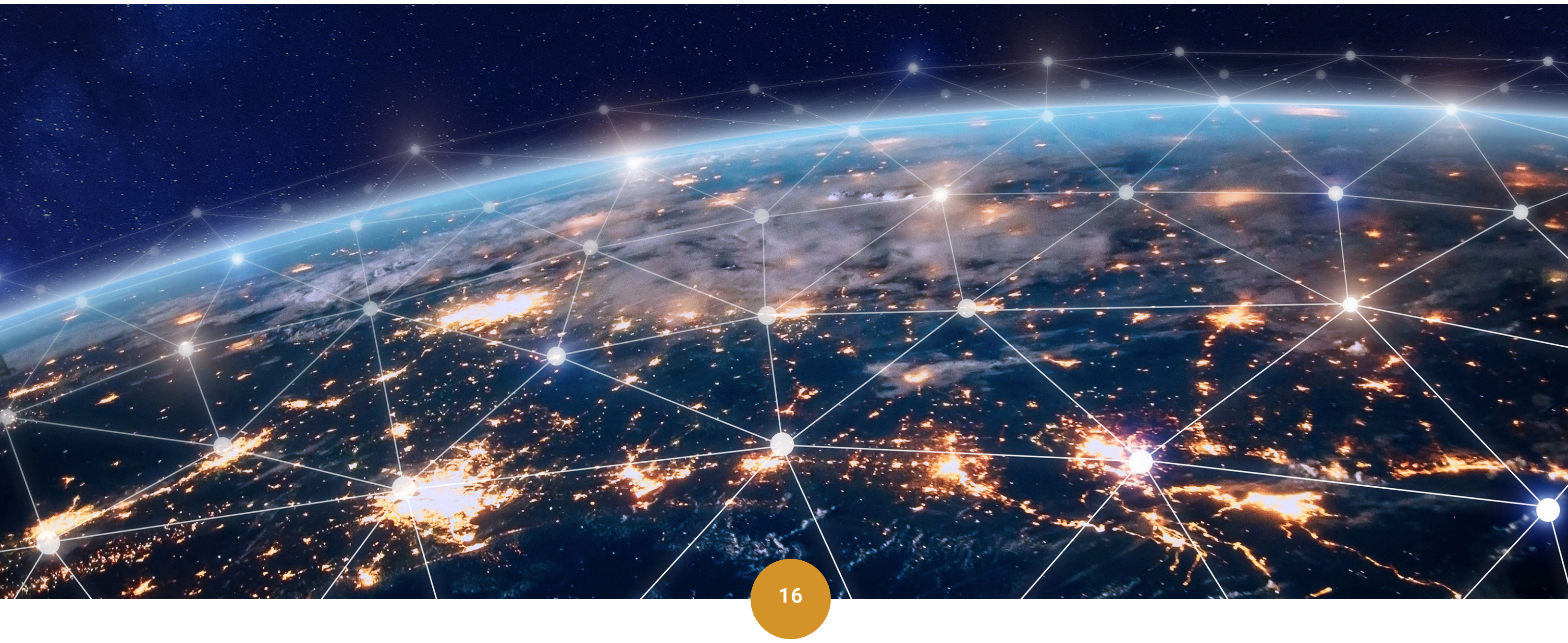
In the 118th Congress, cybersecurity must continue to be a top priority for our congressional leaders, and it is essential that we continue to advance legislation that ensures our digital future. Only then can we have confidence in a safe and secure future.

The NTSC will continue to advocate for cybersecurity legislation tailored to effectively address the cybersecurity needs of our communities, our organizations, and our country. Moreover, the NTSC believes cyber policy should be developed in collaboration with experts, stakeholders, and government officials to ensure that they are effective and accurate. Amidst a constantly evolving threat landscape, cyber experts should be consulted to ensure that policies and legislation are comprehensive and up to date.

Key issues the NTSC will be focused on in 2023 include:

- Harmonizing the various cyber incident reporting legislative efforts to ensure there is one standard for businesses to follow.
- Passing a federal privacy mandate that establishes a national standard.
- Establishing a holistic national cyber workforce development strategy.
- Establishing a “secure by design” policy for all technology and software.
- Continuing the effort to establish a cyber threat intelligence program that provides contextual and timely information to both the public and private sectors.
- Strengthening the public/private partnership.

Finally, it is important to recognize cybersecurity is a shared responsibility, and all stakeholders must work together to create effective policies that protect individuals, businesses, and governments. Cybersecurity is an essential part of all of our lives, and in this increasingly interconnected global economy, cyber policy and legislation are essential components of protecting it.



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