Center for Internet Security®

Confidence in the Connected World™

Year in Review

2018

Welcome Message

In 2018, CIS once again demonstrated the importance of our role as an independent, global leader in cybersecurity.

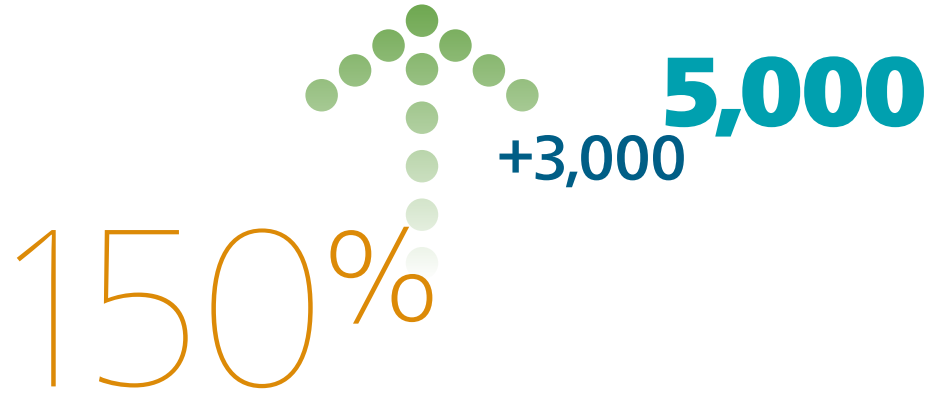
Among our most notable accomplishments was the creation of the Elections Infrastructure Information Sharing & Analysis Center® (EI-ISAC®). Using the guiding principle of "We can achieve more collectively," CIS entered the election security arena with the EI-ISAC in March. In a parallel landmark development, CIS led the collaborative production of *A Handbook for Elections Infrastructure Security* to help election officials and their technical support teams defend U.S. election systems and networks vital to our functioning democracy.

Albert
CIS Network Monitoring

Throughout the remainder of 2018, the EI-ISAC grew to include all 50 states and almost 1,500 total members, including many local election officials and their technical staff members, election technology vendors, and federal partners. In 10 scant months, the EI-ISAC became the fastest-growing ISAC in history. The EI-ISAC also deployed network monitoring sensors, called "Albert sensors," to help protect the most critical elements of our election infrastructure.

By sharing information about the threat landscape, monitoring network activity for malicious traffic, educating election officials about cybersecurity, and identifying necessary technical cybersecurity controls, the EI-ISAC helped the U.S. election community make substantial strides toward ensuring the security and integrity of our elections.

During the primaries and mid-term elections, the EI-ISAC sponsored an online National Cyber Situational Awareness Room, which connected election offices across the nation with the U.S. Department of Homeland Security, the FBI, and the EI-ISAC Security Operations Center. The Situation Room provided real-time awareness of cyber threats as well as physical incidents.



MS-ISAC®

During 2018, the Multi-State Information Sharing & Analysis Center® (MS-ISAC®) added more than 3,000 new members to reach 5,000 members. Overall membership saw a 150 percent increase. MS-ISAC municipal government members now cover 80 percent of the U.S. population. Our partnership with state and local government organizations and the Department of Homeland Security continues to grow stronger with increased depth and breadth of the intelligence provided through the MS-ISAC monitoring, information sharing, and cyber education missions.

CIS also greatly expanded the quality and quantity of our product offerings this year. In January 2018, CIS launched an effort to provide complimentary CIS SecureSuite® subscriptions to all U.S. state, local, tribal, and territorial governments. These organizations now have access to this suite of powerful tools and CIS support services, which will simplify implementation and enforcement of high priority security controls.

CIS SecureSuite®

CIS Hardened Images™

+160 million hours

In 2018, the number of CIS Hardened Images™ available for Amazon Web Services®, Microsoft® Azure, and Google Cloud® platforms was significantly increased. Cloud customers used more than 160 million machine hours of CIS Hardened Images in 2018. These cloud services have emerged as our fastest-growing and most impactful products.

The CIS Controls™ continue to set the standard for best practices in cyber defense as recognized by leading organizations around the world. Global recognition included the European Telecommunications Standards Institute, now globally known as ETSI, updating its compendium of Technical Reports to include the CIS Controls. In addition, the Aerospace Industries Association (AIA) embraced the CIS Controls as the basis for their Cyber Standard Practice document.

CIS Controls™

Numerous additions were made to the portfolio of companion guides for these CIS best practice standards, including the *Implementation Guide for Industrial Control Systems*, which provides cyber defense guidance for Industrial Control System environments. In addition, CIS released the CIS Risk Assessment Methodology (CIS RAM), to assist organizations in assessing overall organizational cyber risks. To date, the CIS Controls have been downloaded more than 157,000 times.

157K Downloads

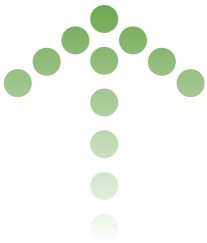
CIS RAM

These 2018 achievements reflect the unwavering commitment by the CIS team to help safeguard organizations of all sizes against cyber threats—in short, to continue our mission to deliver *Confidence in the Connected World.*

Sincerely,

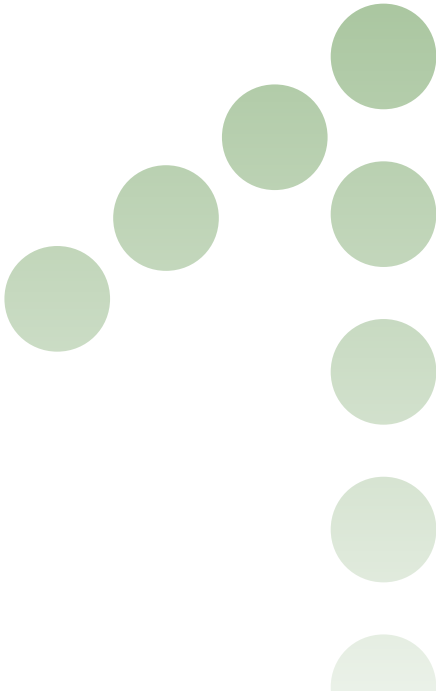
John M. Gilligan
CEO and President

At a Glance



36%

CIS grew its workforce by 36 percent



CIS implemented a new performance management system that supports engagement and professional development

TOP WORK PLACES 2018

TIMES UNION
timesunion.com

CIS was named a Top Workplace by the *Albany Times Union*

CIS Benchmarks

1M+

CIS Benchmarks downloads

32

CIS Benchmarks developed or updated

CIS Benchmarks™

31

CIS Benchmarks developed or updated in formats to support assessment and implementation

148

CIS Benchmarks publicly available

30+

Active CIS Benchmarks in communities covering multiple technology platforms

CIS SecureSuite

6,800+

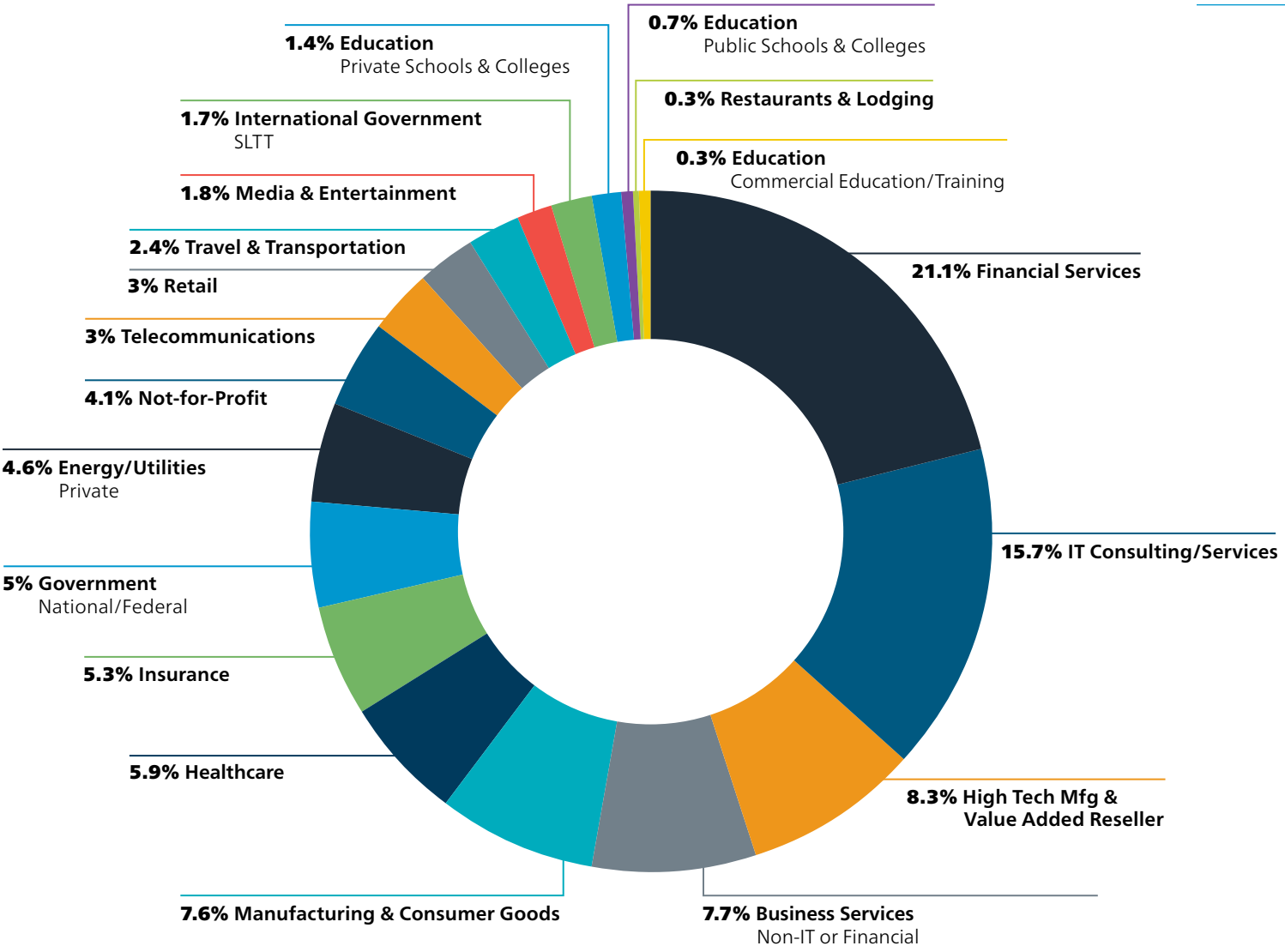
SecureSuite membership increased to more than 6,800 members in 2018.

CIS SecureSuite®

CIS Services®

CIS Services provided vulnerability assessments, and managed security services, social engineering/ phishing services, and penetration testing services

2018 CIS SecureSuite Members by Industry*



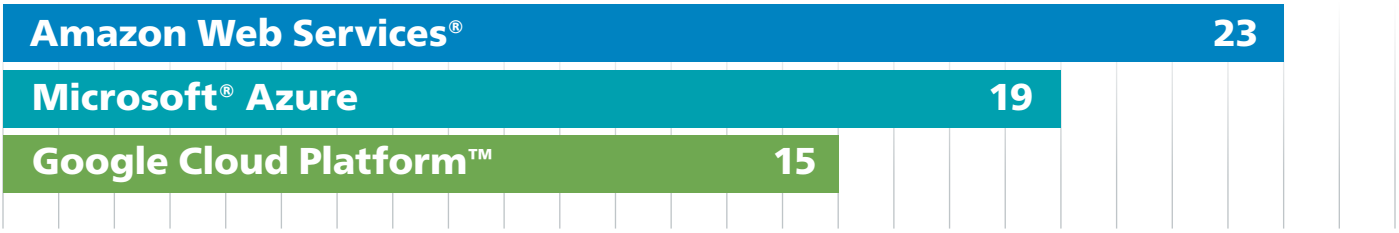
* Percentages above exclude U.S. state, local, territorial and tribal governments and public academic institutions

CIS Hardened Images

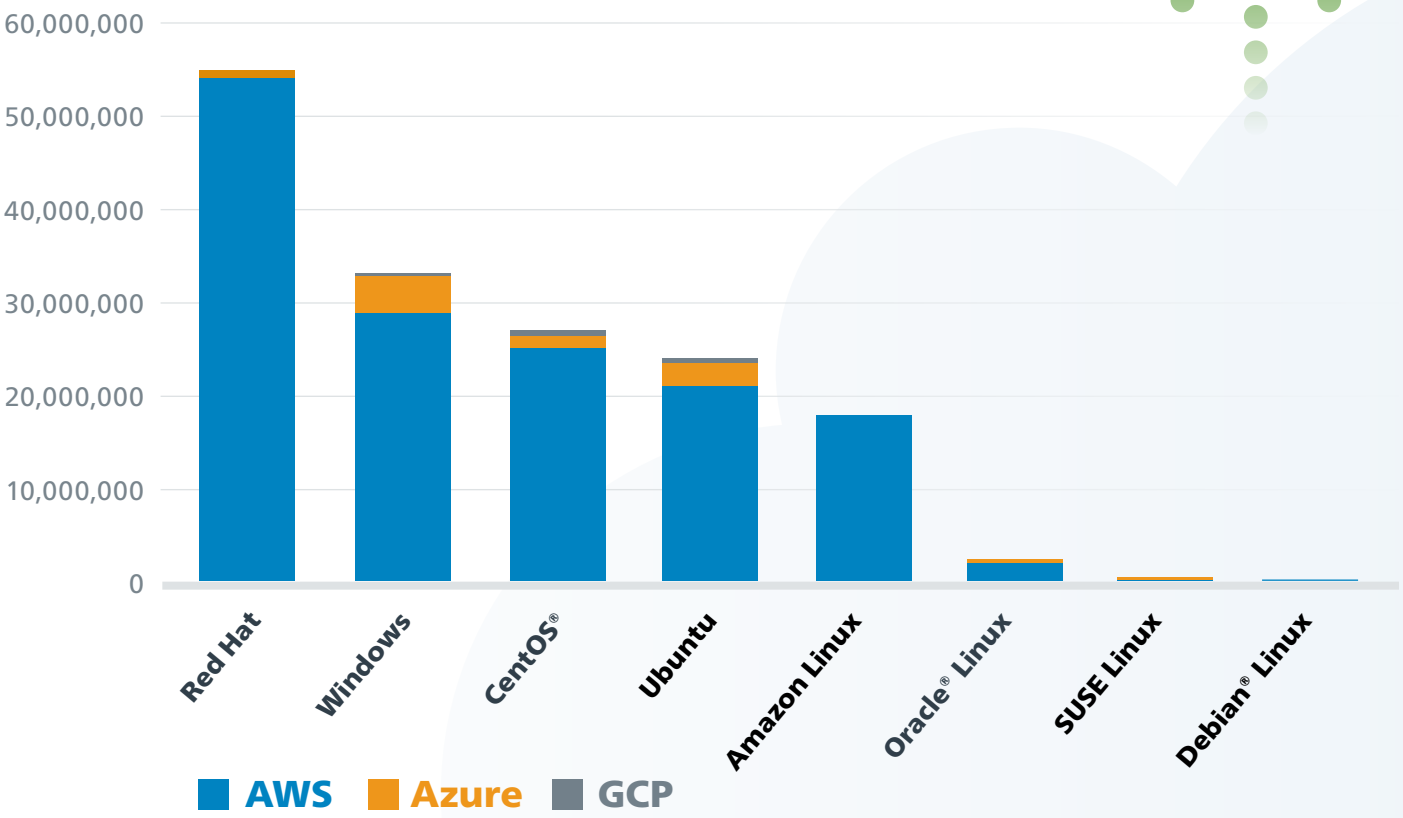
CIS Hardened Images™

CIS became the Seller of Record for CIS Hardened Images™ in the AWS Marketplace® in 2018. CIS expanded offerings in the AWS Marketplace to include CIS Hardened Images for Ubuntu® 18.04 and Amazon Linux® 2. CIS also released our first container base image using Ubuntu 16.04. CIS Hardened Images for Red Hat® Enterprise Linux 6 and 7, SUSE® Linux 12, and Ubuntu 18.04 were released in the Microsoft® Azure Marketplace. Additionally, CIS Hardened Images for SUSE Linux 11 and 12 and Ubuntu 18.04 were released in Google Cloud Platform™.

Current number of CIS Hardened Images by provider:



2018 Combined CIS Hardened Images Hours and Usage by Technology



CIS Controls

Overview

Developed by a global community of experienced IT practitioners, the CIS Controls are a technology- and vendor-independent set of concise, prioritized cybersecurity actions and best practices. The CIS Controls team successfully increased global awareness and adoption of this actionable set of best practices, while simultaneously producing extensive new guidance content in 2018.

Program Accomplishments

The CIS Controls Version 7 was launched in the first quarter of this year. New features in CIS Controls Version 7 include:

- Improved consistency and simplification of the wording of each Sub-Control
- Implementation of "one ask" per Sub-Control
- More focus on authentication, encryption, and application white listing
- Better accounting for security technology and emerging security problems
- Better alignment with other frameworks (such as the NIST CSF)
- Supports the development of related products (e.g., measurements/metrics, implementation guides)
- Identifies types of CIS Controls (basic, foundational, and organizational)

Paraguay Government

The government of Paraguay formally approved the use of CIS Controls Version 7 as the cybersecurity baseline for all government institutions. Implementation of the CIS Controls 1-6, considered the basic Controls, will start in February 2020. The goal is full implementation of all CIS Controls by 2024.

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

V7

- **CIS Controls V7 Measures and Metrics** – The CIS Controls are organized in a hierarchal structure. There are 20 Controls that are further divided into 171 Sub-Controls. As more organizations are adopting this set of best practices, there is an increased interest in being able to measure and manage their implementation of the 171 Sub-Controls. CIS Controls V7 Measures and Metrics addresses how to measure if a Sub-Control has been implemented successfully based on Six Sigma levels. Six Sigma is a data-driven approach to quality, which works to reduce variation and the associated defects, wastes, and risks in any process.

- **The CIS Controls team started work with the University of North Carolina at Charlotte** to develop criteria for objectively measuring each of the 171 Sub-Controls. The primary focus will be on measuring the different levels of the three implementation groups. This work will pave the way for the future creation of automated tools that will measure the CIS Controls implementation.

MS-ISAC

MS-ISAC®

800+

Distributed more than 800 products to members

75,571

Sent 75,571 network monitoring and system compromise/vulnerability notifications to members

317 17.7 trillion

Analyzed 317 petabytes of data, which generated 17.7 trillion records

239

Conducted 239 forensic investigations

18,300+

Analyzed over 18,300 pieces of suspected malware

The Multi-State Information Sharing & Analysis Center (MS-ISAC), with financial support from the Department of Homeland Security, continued its mission to improve the cybersecurity posture of the nation's state, local, tribal, and territorial (SLTT) governments through focused cyber threat identification, protection, detection, response, and recovery activities this year. Individual sectors within our membership all saw marked increases in growth throughout the year. MS-ISAC tribal government membership increased by 81 percent, K-12 schools by 333 percent, and public utilities by 125 percent.

MS-ISAC also runs the Nationwide Cybersecurity Review (NCSR), which provides insight on the level of maturity and risk awareness of the SLTT's information security programs from year to year. DHS and MS-ISAC use the results of this report to work on improving the cybersecurity of the SLTT community.

669 SLTT Entities

The results of the 2018 NCSR are based on participation from 669 SLTT entities in 43 states. They include 277 local governments (representing 43 states), six tribes, and 343 state agencies (representing 24 states). An analysis of this year's results showed that state, local, and tribal peer groups continued to report overall scores which fell below the recommended minimum maturity level.

All NCSR participants continue to identify the same top five security concerns over the past four years:

- Lack of sufficient funding
- Increasing sophistication of threats
- Lack of documented processes
- Emerging technologies
- Inadequate availability of cybersecurity professionals

The MS-ISAC national meeting was held in New Orleans, where over 380 members from across the nation came together.

Elections Infrastructure ISAC®

EI-ISAC

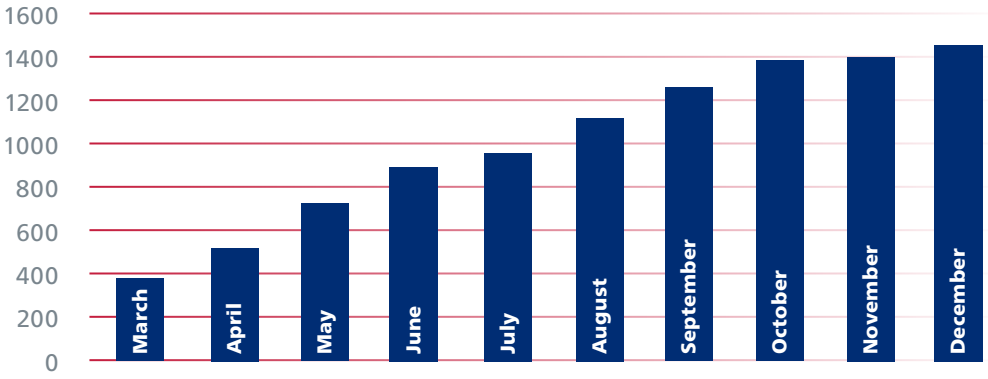
The EI-ISAC is a voluntary and collaborative effort based on a strong partnership between CIS, the DHS Cybersecurity and Infrastructure Security Agency (CISA), and the Election Infrastructure Subsector Government Coordinating Council (EIS-GCC).

During 2018, the EI-ISAC evolved from an idea to a formalized collective of dedicated election officials, their staff members, associations, technology vendors, federal partners, and cybersecurity experts working tirelessly to help secure the U.S. elections infrastructure.

The EI-ISAC was conceived as a means of leveraging the many capabilities and the infrastructure of the MS-ISAC. The integration of the two continued after the EI-ISAC's formal launch in March. Both the MS-ISAC and EI-ISAC benefit by operating under the auspices of CIS. This allows them to work together to educate and protect SLTT governments from the myriad cyber threats that are aimed at both the traditional government IT systems and those specific to elections.

Both ISACs continue to utilize centralized, and in many cases shared, resources to enable a greater level of visibility and information-sharing across the elections and the SLTT government sectors to benefit the constituencies of both organizations. Everything from webcasts to workgroups to in-person meetings integrates the needs of both ISACs, offering efficiency and consistency for the Membership.

2018 EI-ISAC Membership Growth



ISACs Combined Security Best Practice Recommendations and Tools

- Security Operations Center (SOC) providing 24/7/365 incident triage and immediate responses
- Computer Emergency Response Team (CERT) to provide incident responses and forensic services
- Cyber Threat Intelligence Team to provide forward-leaning analysis, written products, and presentations
- Engineering Team to provide sensor deployment and technical assistance
- Stakeholder Engagement Team to provide member support and engagement
- Election-specific and general threat intelligence and vulnerability monitoring
- National Cyber Situational Awareness Room to monitor election activity
- Training sessions and webinars

The EI-ISAC will continue to operate in partnership with members and stakeholders nationwide to ensure the integrity of elections in the United States.

CIS CyberMarket

CIS CyberMarket® continues to serve the U.S. state and local government communities by identifying top-notch cybersecurity vendors, vetting them through the CIS CyberMarket Product Review Board, and then negotiating a significant discount for CIS CyberMarket partners. In 2018, our government partners saved more than $11 million on software and services provided by SANS and other vendors.

CIS continued to expand these partnerships this year by adding solution providers including Belarc and Akamai, who are offering our members new and innovative cyber defense tools.

SANS BELARC Akamai

CIS CyberMarket®

$11 million+ saved

CIS CyberMarket staff also continue to leverage the expertise of our partners and CIS subject matter experts by sharing their knowledge in our *Cybersecurity Quarterly.* This digital publication features articles on how to implement best practices, summaries of recent cyber threats and attacks, and other cyber defense information crucial to state and local governments.

CIS Leadership

Officers & Board of Directors

Officers

William Pelgrin
Chairman
Co-Founder and Partner
CyberWA Inc.

John M. Gilligan
CEO and President
Center for Internet Security

Bruce Moulton
Treasurer
Retired

Deirdre O'Callaghan
Secretary and Chief Counsel
Center for Internet Security

Directors

Jack Arthur
Octo Consulting Group

Dr. Ramon Barquin
President and CEO
Barquin International

Jane Holl Lute

Christopher Painter

Alan Paller
Founder and Director of Research
SANS Institute

Franklin Reeder
Co-Founder
Center for Internet Security

Richard Schaeffer
Advisor
Riverbank Associates LLC

Roberta Stempfley
Director, CERT Division
Software Engineering Institute

Phil Venables
Managing Director and Chief
Information Risk Officer
Goldman Sachs & Co.

Executive Team

Sean Atkinson
Chief Information Security Officer

Brian Calkin
Chief Technology Officer

Carolyn Comer
Chief Human Resources Officer

Gina Chapman
Chief of Staff

Thomas Duffy
Senior Vice President
Operations and Services
Chair, Multi-State ISAC

Curtis Dukes
Executive Vice President
General Manager
Security Best Practices

Meg Keyes
Senior Vice President
Sales and Business Services

Angelo Marcotullio
Chief Information Officer

Tony Sager
Senior Vice President
and Chief Evangelist

Albert Szesnat
Chief Financial Officer

Center for Internet Security®

Twitter
twitter.com/CISecurity

LinkedIn
linkedin.com/company/122681

Instagram
instagram.com/cisecurity

Facebook
facebook.com/CenterforIntSec

YouTube
youtube.com/user/TheCISecurity

31 Tech Valley Drive
East Greenbush, New York 12061
518.266.3460
Fax 518.266.2085
www.cisecurity.org