The Center for Internet Security

The Center for Internet Security (CIS) operates as a 501(c)(3) not-for-profit organization to advance cybersecurity readiness and response for public and private sector enterprises. CIS delivers world-class cybersecurity solutions to help prevent and respond to cyber incidents serving as an authoritative, independent source of cybersecurity expertise to identify, validate, promote, and sustain best practice in cybersecurity and to work collaboratively with others to enable an environment of trust in cyberspace.

In particular, CIS provides secure configuration benchmarks and security automation content and makes available other products and resources that help partners achieve their security goals.

CIS also serves as the home of the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Critical Security Controls.

Find out more information about CIS here: https://www.cisecurity.org/

The Multi-State Information Sharing and Analysis Center

The MS-ISAC is a voluntary and collaborative effort based on a strong partnership with the U.S. Department of Homeland Security (DHS). The MS-ISAC has been designated by DHS as the focal point for cyber threat prevention, protection, response and recovery for the nation's state, local, territorial, and tribal (SLTT) governments as well as Fusion Centers. MS-ISAC's 24x7 cybersecurity operations center provides early cyber threat warnings, threat advisories, vulnerability identification and mitigation, malware and forensic analysis, automated threat feeds and incident response support. MS-ISAC supports information sharing among SLTTs through a broad range of programs, services, and educational forums.

Further, MS-ISAC provides around-the-clock monitoring of many SLTT networks, analyzing over 50 billion logs per week. In 2014 alone, MS-ISAC analyzed, assessed, detected, and reported on over 62,000 malicious activity events. Further, MS-ISAC sent over 14,000 notices to SLTTs identified potential malicious activity on their system and networks.

Find out more information about the MS-ISAC here: https://msisac.cisecurity.org/

Critical Security Controls

CIS is also the home of the Critical Security Controls, the set of internationally recognized prioritized actions that form the foundation of basic cyber hygiene, demonstrated to prevent 80-90% of all known pervasive and dangerous cyber attacks.

The CIS Controls are especially effective because they are regularly updated by a global network of cyber experts based on actual attack data derived from a variety of public and private threat sources.

Essentially, the CIS Controls act as a blueprint for network operators to cut through clutter of innumerable recommendations made by innumerable sources--the “Fog of More”—to improve cybersecurity by suggesting specific actions to be done in a priority order. In this regard, they help all organizations, especially the small- and mid-sized entities that might need help in identifying exactly what to do when.

The California Data Breach Report (2016), recently released by Attorney General Harris, has concluded that the Critical Security Controls constitute a minimum level of information security. The report concludes that failing to implement all relevant Controls "constitutes a lack of reasonable security.” (CA AG data breach report here: https://oag.ca.gov/breachreport2016) (at Recommendation 1)

For quick reference, the Controls are included in the following foundational frameworks, reports, and documents:

- NIST Framework – Appendix A, page 20, and throughout the Framework Core (referred to as "CCS CSC”)
- Symantec 2016 Internet Security Threat Report, https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf, pages 75-77
- Verizon DBIR 2015, page 55
- Tripwire, “The Executive’s Guide to the Top 20 Critical Security Controls,” http://www.tripwire.com/state-of-security/featured/20-csc-list-post/
- Zurich Insurance - page 28
- NGA (National Governors Ass’n), page 4
- UK CPNI (the British infrastructure protection directorate--entire web

page references the Controls)

- Conference of State Bank Supervisors, "Cybersecurity 101: A Resource Guide for Bank Executives, pages 8, 12, 24, https://www.csbs.org/CyberSecurity/Documents/CSBS%20Cybersecurity%20101%20Resource%20Guide%20FINAL.pdf

Find out more information about the Controls and download them for free at: https://www.cisecurity.org/critical-controls.cfm

Attachment 1

MS-ISAC Member Benefits

- **Incident response resources -** A dedicated team is available to assist SLTT 24x7x365
- **Cyber security advisories -** Critical, timely alerts on new and emerging threats and vulnerabilities, these include malware infections, APT attacks, compromised servers and Ransomware
- **Notifications regarding potential compromised systems -** Through its relationships with federal partners and other intel sources, including its own intelligence, the MS-ISAC is able to correlate data and contacts Members when it becomes known their systems may have been compromised
- **Training discounts and opportunities –** Results in saving of up to 85% off the commercial price
- **Daily cyber tips feed -** Highlight good cyber practices and provide guidance on avoiding threats
- **Monthly cyber security newsletters -** Two-page, non-technical bulletin focused on current topics
- **Bi-monthly cyber security webcasts -** Featuring experts who discuss the latest cyber issues
- **Monthly Member webcast meetings –** Discuss latest cyber incidents, national cyber security initiatives, special report-outs from Members, as well training and procurement opportunities
- **Emergency conference calls to brief Members on major threats or reports of Cyber incidents**
- **Access to secure portal for emails and document sharing**
- **Cyber security alert level status map for each state on MS-ISAC secure portal and NCCIC floor**
- **Monthly calls for analysis regarding vendor patch releases**
- **Participation in federal cyber security exercises**
- **Develop and distribute customized Annual Cyber Security Awareness Month materials**
- **Annual in-person Membership meeting -** Tremendous opportunity to meet MS-ISAC colleagues, participate in discussion groups, and learn from experts in the cyber security industry
- **Collective Awareness and Information Sharing –** Increases the value of information by providing awareness at the National level

MS-ISAC Workgroup The workgroups are voluntary committees focused on specific initiatives and deliverables in support of the MS-ISAC mission. All Members are encouraged to join a workgroup. The workgroups serve a significant role in the creation and implementation of MS-ISAC initiatives and provide a tremendous opportunity to collaborate with your peers across the country. Below is a list of MS-ISAC workgroups:

- Cyber Security Metrics
- Business Continuity, Recovery, and Cyber Exercises
- Education and Awareness
- Legislative Awareness and Compliance
- Intel and Analysis
- Industrial Control Systems
- Mentoring Program

National Cyber Security Review

The Nationwide Cyber Security Review (NCSR) is a voluntary self-assessment survey developed in response to the Senate Appropriations Committee request for an ongoing effort to chart nationwide progress in cybersecurity and identify emerging areas of concern. The NCSR, now available annually during October CyberSecurity Awareness Month, is aligned to the NIST CyberSecurity Framework. The NCSR serves as a tool to measure progress in cybersecurity and to drive initiatives and priorities according to the identified needs of the SLTT governments.

Monitoring Services

The MS-ISAC through its 24x7x365 Security Operation Center provides monitoring services along with threat and vulnerability analysis and notifications to SLTT, providing them with an enhanced ability to detect and defend against the latest cyber threats.

These services provide a view of system and network activity that enhanced situational awareness of SLTT networks across the country. The SLTT situational awareness contributes to the national cyber situational awareness prepared by the NCCIC. This collective situational awareness of the overall threat landscape enables the MS-ISAC to better assist all SLTT with threat and migration resources.

Attachment 2

CIS Critical Security Controls

The **CIS Critical Security Controls** are a set of internationally recognized measures developed, refined, and validated by a large community of leading security experts from around the world. They represent the foundational actions of cyber hygiene that every organization could implement to protect their networks to prevent **85% of known vulnerabilities.**

Prioritized Action

The CIS Controls are not just another lis
instead represent a concis
align with other security frameworks, including the
NIST -CERT Cybersecurity Framework, US recommendations,
and international gu
on a smaller number o
common attack patterns. Vetted across a broad community of government and industry, with very strong consensus on the resulting set of controls, they serve as the **basis for immediate high-value action.**

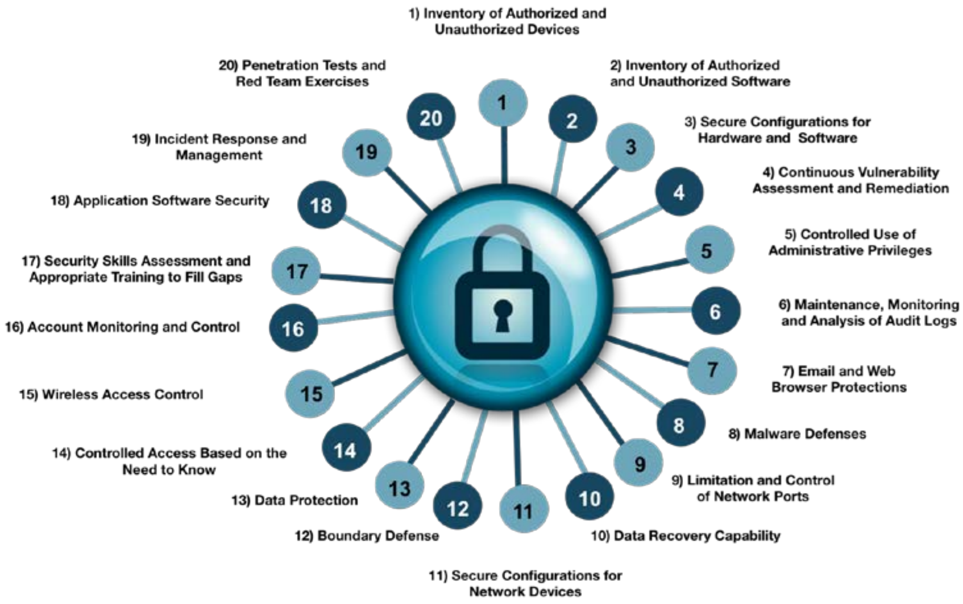
Community-based Approach

The **Center for Internet Security** regularly convenes experts to refine, update and validate the CIS Controls, and collaborates with public and private partners globally to promote their adoption and implementation. The experts on the CIS Controls panel help ensure the CIS Controls represent the community's best insight into threat, vulnerability, and defensive technology, as well as ensure that the CIS Controls can be **supported through cost-effective solutions.**

MAKING BEST PRACTICE COMMON PRACTICE

Download the CIS Critical Security Controls at

http://www.cisecurity.org/critical-controls.cfm The Center for Internet Security 1700 N. Moore Street, Suite 2100 Arlington, Virginia 703-600-1935 www.cisecurity.org


1) Inventory of Authorized and Unauthorized Devices
2) Inventory of Authorized and Unauthorized Software
3) Secure Configurations for Hardware and Software
4) Continuous Vulnerability Assessment and Remediation
5) Controlled Use of Administrative Privileges
6) Maintenance, Monitoring and Analysis of Audit Logs
7) Email and Web Browser Protections
8) Malware Defenses
9) Limitation and Control of Network Ports
10) Data Recovery Capability
11) Secure Configurations for Network Devices
12) Boundary Defense
13) Data Protection
14) Controlled Access Based on the Need to Know
15) Wireless Access Control
16) Account Monitoring and Control
17) Security Skills Assessment and Appropriate Training to Fill Gaps
18) Application Software Security
19) Incident Response and Management
20) Penetration Tests and Red Team Exercises
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20