Testimony of Steve Spano
President and Chief Operating Officer
Center for Internet Security
Hearing on "Enhancing Preparedness and Response Capabilities to Address Cyber Threats"
Subcommittee on Emergency Preparedness, Response, and Communications and Subcommittee on Cyber Security, Infrastructure Protection, and Security Technologies
Committee on Homeland Security
U.S. House of Representatives
311 Cannon House Office Building
Tuesday, May 24, 2016, 10:00 a.m. ET

Chairmen Donovan and Ratcliffe, Ranking Members Payne and Richmond, and members of the Committee, thank you for inviting me today to this hearing. My name is Steve Spano, and I serve as the President and Chief Operating Officer of the Center for Internet Security—or "CIS." I appreciate the opportunity today to share our thoughts on the current state of national cybersecurity, focusing in the area we know best: State, Local, Tribal and Territorial (SLTT) government entities. As the nation addresses the complicated issue of cybersecurity, your efforts to assess the current state of national cyber preparedness and response capabilities and determine how best to improve our national cybersecurity posture is noteworthy. I look forward to offering our ideas on how we can collectively build on the progress being made in this important area of critical national security.

Established in 2000 as a not-for-profit organization, CIS's primary mission is to advance cybersecurity readiness and response. CIS was instrumental in establishing the first guidelines for systems hardening at a time when there was little online security leadership. In 2010, the U.S. Department of Homeland Security (DHS), under the National Protection and Programs Directorate (NPPD), partnered with CIS to host the Multi-State Information Sharing and Analysis Center, or MS-ISAC. Under a cooperative agreement with DHS, the MS-ISAC was established as a 24x7 cybersecurity operations center that provides real-time network monitoring, threat analysis, and early warning notifications to SLTTs. MS-ISAC also consolidates and shares threat intelligence information with the DHS National Cybersecurity and Communications Information Center (NCCIC), where we have two employees serving as liaisons for MS-ISAC. In 2015, we became the home of the CIS Critical Security Controls, previously known as the SANS Top 20. With this expanded operational mission, CIS has evolved as a trusted resource to help public and private organizations start secure and stay secure.

Today, CIS collaborates with the global security community to lead government and private-sector entities to online security solutions and resources. While I will elaborate more fully below, the 100-plus professionals at CIS provide cyber

expertise in three main program areas:

1. As I just mentioned, the MS-ISAC operates a 24x7 Secure Ops Center to support SLTTs.

2. The CIS Critical Security Controls (CIS Controls), a consensus-driven, prioritized set of cyber best practices created to stop today's most pervasive and dangerous cyber attacks. The CIS Controls are referenced in several policy and security frameworks such as the NIST 800.43; and

3. The Security Benchmarks, a program that provides well-defined configuration best practices to help organizations worldwide assess and improve their cybersecurity. Over 100 consensus-based Security Benchmarks have been developed to date, and Security Benchmarks members can access tools and automated content for both traditional hardware and software as well as cloud-based services.

More information about CIS is included at Attachment A and incorporated herein by reference.

(1) The Current State of Cybersecurity Preparedness

CIS's assessment of the current state of cybersecurity preparedness and response capabilities is based on our collective daily experience with the MS-ISAC, represented by over 1,000 SLTT members (including all 50 states), as well as our dealings with those using the CIS Security Benchmarks and the CIS Controls, all of which provide us unique and wide-ranging insight into the cybersecurity posture of those we serve.

Today, thanks to Congressional and DHS support and SLTT participation, the MS-ISAC is actively monitoring the networks of 41 states and territories. In 2016, our goal is to have all 50 states and all 6 territories being monitored by the MS-ISAC. Our members represent local governments, public universities, critical infrastructure entities, and public authorities that own and operate critical infrastructures. In 2015, our monitoring program analyzed over 3 trillion records, which generated over 56,000 actionable alerts to our SLTT partners. In 2015, our CERT team managed 161 incidents for our partners, largely focused on computer forensics. Their efforts actively identify types of threats, origins of attack, and root causes of the attack. Our intelligence team has produced a large number of analytical reports that both DHS and the FBI have cited as key resources to help in their investigations and high-level threat detection. Our cyber support for SLTTs also includes a computer emergency response capability, and the issuance of real-time cyber alerts, advisories, and intelligence products.

Based on this work, we can state that since 2004, when the MS-ISAC partnership with DHS began, we have seen progress in the state of cybersecurity of our

SLTT partners that can be characterized as improving, with many positive trends. There are, however, significant challenges that we are collectively working to improve. These challenges include under-resourced cybersecurity budgets, poorly crafted and vulnerable software provided by vendors, misconfigured networks, and insufficient numbers of qualified professional staff.

Our assessment of SLTT cybersecurity preparedness and response capability is supported in the findings of the DHS-funded Nationwide Cyber Security Review (NCSR). This annual review, tasked to the MS-ISAC by DHS, is produced in conjunction with the National Association of Counties and the National Association of State Chief Information Officers, and is reported to Congress by DHS every two years. It is a voluntary, self-assessment survey designed to evaluate cyber security management within, and the cybersecurity posture of, SLTT governments. To gauge the nationwide level of cybersecurity readiness, the NCSR measures maturity of cybersecurity programs within the SLTT community by assessing how SLTTs are performing in 13 key cybersecurity areas. The 2013 and 2014 NCSRs found SLTT respondents continuing to improve towards the highest level of maturity, "risk aware", in all 13 of these measured functions, but they have not yet reached that maturity level in any of the 13 categories. Further support for our assessment is found in the DHS 2015 National Preparedness Report (the "Preparedness Report"), which acknowledges both that SLTTs place significant emphasis on the importance of cybersecurity, but have been challenged to find sufficient financial resources and staffing to meet growing cybersecurity demands.

The MS-ISAC, the NCSR and the Preparedness Report all recognize that steady progress is being made in many areas of SLTT cybersecurity, in the face of cyber threats that continue to increase in scope, sophistication, and number, but that challenges remain for SLTTs to reach full cybersecurity preparedness. This reality will not change any time soon. The strategy and execution of defensive responses must evolve at a faster pace. This will require continued investment, strong leadership, and collaboration at all levels of government.

Outside of the SLTT space, our experience with our Security Benchmarks customers and those using the CIS Controls also show increased efforts to improve organizations' cybersecurity posture. In the last three years, the number of organizations purchasing Security Benchmarks memberships has almost tripled, and the growth in the use of automated machine image versions of the Benchmarks has grown tenfold since they were first released a year ago. This shows us that there is increasing emphasis on ensuring that organizational networks and devices are securely configured.

In October 2015, we released Version 6 of the CIS Controls. In the period of time since the release, the CIS Controls have been downloaded over 32,000 times. This data, coupled with ongoing requests for information and assistance in learning more about the Controls, shows us that companies and organizations are seeking guidance in how to start secure and stay secure, and are looking for the roadmap to tell them how to

get there.

(2) How CIS is Working to Increase Cybersecurity Preparedness

Since its inception, CIS's mission has been focused on increasing cybersecurity preparedness, both for SLTT governments through the MS-ISAC and for the private sector as well with the CIS Controls and Security Benchmarks programs. I appreciate the opportunity to highlight our work in these three areas, and why we believe our work is making a difference**.**

MS-ISAC

The ongoing work of the MS-ISAC has and will continue to improve the cybersecurity posture of SLTT governments. Our continuous monitoring of SLTT networks across the country provides us with the ability to see and analyze the scope of potential malicious activity and identify when there are multiple incidents of the same nature and source. As noted above, in 2015 alone, MS-ISAC detected and analyzed malicious activity events that generated over 56,000 incident reports. We provide response assistance if needed, including CERT team assistance. Equally importantly, we provide timely issue alerts to all our SLTT members, which include steps to take to avoid or mitigate the risk of the identified malicious activity event. We also share SLTT event information with federal agencies and other trusted partners through our liaisons on the NCCIC floor, so our work also informs the cybersecurity posture of the Federal government and the nation as a whole.

In addition to our monitoring and response services, we produce a monthly situational awareness report that shares timely cybersecurity information with our over 1,000 members. We distribute weekly reports of cyber threat indicators and support an automated indicator sharing platform (STIX/TAXII). We hold monthly webcasts focusing on particular cybersecurity issues. We also offer group purchasing opportunities for cybersecurity training and products, with substantially discounted pricing for SLTTs, educational and not for profit entities. Since starting the purchasing alliance in 2012, we have been able to save SLTT governments almost $30 million in their purchase of essential cybersecurity training and products. Our work with the NCSR is providing SLTTs with a tool to monitor and track their progress, both internally and against other SLTT entities.

More information on MS-ISAC services is included in Attachment B and incorporated herein; further information is available here: https://msisac.cisecurity.org/.

CIS Critical Security Controls

CIS is 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 were initially created, and 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, so they are informed by both professional expertise and real world threat information.

The CIS Controls act as a blueprint for network operators to improve cybersecurity by suggesting specific actions to be done in a priority order. In this regard, we strongly believe that the CIS Controls can help all organizations, especially the small- and mid-sized entities, many of which need help in identifying exactly what to do and when.

The CIS Controls are recognized by a number of cybersecurity frameworks and reports as an effective and practical tool for improving an organization's cybersecurity preparedness. The CIS Controls are specifically called out in the NIST Cybersecurity Framework as one of a handful of cybersecurity tools that help organizations implement the Framework. Just recently, the California Attorney General released the California Data Breach Report (2016), which specifically points to the Controls as a tool that if followed, would meet the requirement of "reasonable security" under California law. (The full report can be accessed here: https://oag.ca.gov/breachreport2016).

Additionally, the Controls are included in the following foundational frameworks, reports, and documents:

- NIST Framework
- 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/Atlantic Council "Risk Nexus: Overcome by Cyber risks? Economic Benefits and Costs of Alternate Cyber Futures"- page 28
- NGA "National Governors Association Call to Action on Cybersecurity", 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

We make the CIS Controls available for download at no cost to the general public, as well as free companion guides that provide more detailed information and support for the implementation of the CIS Controls. Find out more information about the

Controls and download them for free at: https://www.cisecurity.org/critical-controls.cfm. Additional information about the CIS Controls is also included at Attachment C and incorporated herein by reference.

CIS Security Benchmarks

CIS is also the world's largest producer of authoritative, community-supported, and automatable security configuration benchmarks and guidance. The CIS Security Benchmarks (also known as "configuration guides" or "security checklists") provide highly technical, detailed security recommendations for specific components of information technology, such as operating systems and devices, and are vital for any credible security program. The Security Benchmarks are developed though a collaborative effort of public and private sector security experts. CIS has developed over 100 consensus-based Security Benchmarks have been developed today and are available in PDF format free to the general public, or in an automated format through the purchase of a membership. We have also created a number of Amazon Machine Images® (AMIs) for the most utilized Security Benchmarks, which are available for purchase in the AWS Marketplace® and in Amazon GovCloud®, and we are discussing similar arrangements with other cloud providers. CIS Security Benchmarks are used worldwide by organizations ranging from small, nonprofit businesses to Fortune 500 companies.

The CIS Security Benchmarks are referenced in a number of recognized security standards and control frameworks, including:

- Payment Card Industry (PCI) Data Security Standard v3.1 (PCI) (April 2016)
- NIST Guide for Security-Focused Configuration Management of Information System
- Federal Risk and Authorization Management Program (FedRAMP) System Security Plan;
- DHS Continuous Diagnostic Mitigation Program; and
- CIS Critical Security Controls, Version 6©

More information about CIS Security Benchmarks is included at Attachment D and incorporated herein by reference.

(3) What More Can Be Done?

The current cyber threat is clear, unmistakable, and unlikely to abate anytime soon. Fortunately, much is currently being done to improve cybersecurity—but more needs to be done. We would like to focus our comments on two areas that we believe are of significant importance to both SLTT and non-SLTT organizations: (1) improving cyber hygiene; and (2) creating a comprehensive approach to both increasing and improving the cybersecurity workforce.

Improving Cyber Hygiene

Probably the single most important effort that we can undertake to dramatically make our networks more secure is to adopt basic cyber hygiene. Like personal hygiene, it involves basic, regular routines and actions that are needed to maintain basic safety and security.

Despite a growing understanding of the threats and vulnerabilities in the technical community, widespread adoption of safe cyber behavior in cyberspace is the exception, not the norm. It is our experience that the vast majority of cyber incidents result from either the failure to patch known vulnerabilities in software and web applications or failure to adopt proper security configurations on network operating systems or devices.

We believe that part of the difficulty in getting more traction for cyber hygiene is the existence of a plethora of defensive tools, security frameworks, and guidelines, combined with the complexity of our networks, which have simply overwhelmed and confused consumers, private sector companies and governments. For example, while the NIST Framework lays out a process for beginning a dialogue on cyber security measures, it is by design not a framework listing prioritized actions based on effectiveness.

As we have discussed above, we believe that the CIS Controls provide the specific, actionable controls in priority order that will thwart the most pervasive attacks. This is supported in a study by the Australian government Department of Defense, which revealed that 85% of known cybersecurity vulnerabilities can be mitigated by deploying the Top 5 CIS Controls. Whether by using the CIS Controls or some other framework, increased efforts by the Federal government to promote a roadmap for basic cyber hygiene will yield proven results in mitigating the most prevalent and pervasive cyber attacks.

Creating a Comprehensive Approach to Improving our Cybersecurity Workforce

One of the major reasons that organizations have struggled in achieving basic cyber hygiene is the lack of available and qualified cybersecurity professionals to undertake the necessary cyber protection actions, particularly on an ongoing basis. There are simply too few qualified cyber professionals in the workforce. This is the result of several factors:

- too few students in the K-12 level of education are interested in pursuing further education in computer science and cybersecurity;
- too few universities and colleges are offering cybersecurity degree or certificate programs that offer the practical training needed to meet the qualifications of cybersecurity professional roles;
- there is a need for more continuing cyber education of staff in the current cybersecurity workforce to keep up with the ever changing technical landscape of cyber threats; and

- for SLTTs and smaller organizations, the ability to hire from the limited existing cybersecurity workforce is hampered by the inability to compete with private sector salary levels.

We believe that there are several areas in which the Federal government can assist with increasing and improving the cybersecurity workforce:

1. Help to increase awareness and promote STEM education at the K-12 level;

2. Because of our DHS support, CIS is able to recruit students from the National Science Foundation's Scholarship for Services Program (SFS) for certain MS-ISAC positions. This program has been a great tool in helping us recruit and maintain entry-level cyber professionals. We would recommend considering additional funding for the SFS program to open the program up to more students. This would assist in growing the number of students entering cybersecurity studies at the college level. We would also suggest considering broadening the organizations that qualify to hire SFS students to include non-governmental critical infrastructure organizations and not for profits, all of whom share the same challenges that Federal and SLTT governments face in recruiting and retaining cyber talent.

3. Providing more opportunities for cyber exercises and simulations and expand participation by SLTT entities. In addition to allowing SLTTs more opportunities to assess their cyber readiness and response capabilities, these exercises and simulations provide ongoing training for the SLTT cybersecurity workforce.

The threat to our nation is real and extends down to every individual. As such, improving our cybersecurity defense of this country demands the combined efforts of us all. We will continue our efforts at CIS to help SLTTs protect citizen data at every level of government. We will also continue our excellent partnership with the federal government as we work to extend monitoring services to all 56 states and territories as the foundation of best practice in cybersecurity information sharing.

I want to thank the committee for the opportunity to participate in this important hearing, and look forward to addressing any questions you might have.

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

Attachment A: The Center for Internet Security
Attachment B: MS-ISAC
Attachment C: CIS Critical Security Controls
Attachment D: CIS Security Benchmarks

Attachment A

CIS Overview

Who We Are

At The Center for Internet Security (CIS), we believe that everyone deserves a secure online experience. CIS harnesses the power of a global IT community to safeguard private and public organizations against cyber threats.

As a 501(c)(3) organization, CIS works to deliver confidence in the connected world. Utilizing its strong industry and government partnerships, CIS combats evolving cybersecurity challenges on a global scale and helps organizations adopt key best practices to achieve immediate and effective defenses against cyber attacks. CIS is home to the Multi-State Information Sharing and Analysis Center (MS-ISAC), CIS Security Benchmarks, and the CIS Critical Security Controls.

How We Do Business

- Cultivate a trusted, collaborative environment for information sharing
- Develop industry-leading, cost-effective cyber security resources
- Provide immediate, effective defenses against cyber attacks

> ***"CIS is not one vendor but a whole community… they represent the Internet of people, working together for a common goal, which is the best way to be secure. CIS is an objective, independent voice in security."***
>
> **- Chief Information Security Officer**
> **Financial Institution**

Who We Serve

State & Local Governments • Small, Medium & International Businesses • Nonprofits

What We Provide

MS-ISAC

The focal point for cyber threat prevention, protection, response and recovery for nation's state, local, tribal, and territorial (SLTT) Governments. The MS-ISAC's 24x7 cybersecurity operations center provides real-time monitoring, threat warnings and incident response

CIS Security Benchmarks

Well-defined, consensus-based, internationally-recognized industry best practices to help assess and improve network cybersecurity. With Membership, organizations receive the Security Benchmarks plus an automated assessment tool and content, security metrics, and more

CIS Critical Security Controls™

A threat-prioritized set of policy-level controls developed by leading cybersecurity experts, widely used as the foundation of organizational cyber security. Distills common security practices into a scalable, actionable list

CIS Aggregate Purchasing

Serves SLTT governments and not-for profit entities to improve cyber security through cost-effective group procurement

CIS Services

Additional services such as vulnerability assessment, incident response, phishing exercises, and monitoring (monitoring available to public entities only)

Learn more about CIS at www.cisecurity.org

Attachment B

MS-ISAC

Who We Are

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a voluntary and collaborative effort based on a strong partnership between The Center for Internet Security (CIS) and the Office of Cybersecurity and Communications within the U.S. Department of Homeland Security (DHS). The MS-ISAC has been designated by DHS as the key resource for cyber threat prevention, protection, response and recovery for the nation's state, local, territorial and tribal (SLTT) governments. Through its state-of-the-art 24/7 Security Operations Center, the MS-ISAC serves as a central resource for situational awareness and incident response for SLTT governments. *There is no cost to be a member.*

Membership Benefits

- 24/7 security operations center
- Cyber security exercises
- Cyber security advisories & daily tips
- Cyber event notifications
- Awareness/education materials
- Network monitoring
- Vulnerability assessment services
- Secure portals for communication & document sharing
- Malicious Code Analysis Platform (MCAP)
- Monthly newsletters, webcasts, & threat briefings
- Alert status map
- Incident response resources
- Discounts on CIS Security Benchmarks
- Discounts on training
- Nationwide Cyber Security Review (NCSR)
- Vulnerability Management Platform (VMP)

"The Multi-State Information Sharing and Analysis Center (MS-ISAC)…allows the Federal Government to quickly and efficiently provide critical cyber threat, risk, vulnerability, and mitigation data to state and local governments."

- U.S. DHS Secretary Janet Napolitano
March 2013

Learn more about the MS-ISAC at https://msisac.cisecurity.org

MS-ISAC Frequently Asked Questions

Who can join the Center for Internet Security's MS-ISAC?
Membership is open to all U.S. SLTT government entities involved in cyber security and/or critical infrastructure protection.

Who are the members?
The MS-ISAC currently includes representatives from all 50 states, all 50 state capitals, all 78 Fusion Centers, hundreds of local governments, several tribal governments and U.S. territories. There are a total of 997 MS-ISAC member organizations across a diverse group of public sectors that includes government, education, utilities, transportation, and more.

What does it cost to join the MS-ISAC?
There is no cost to join the MS-ISAC. It is primarily supported by the DHS to serve as the central cyber security resource for the nation's SLTT governments. The MS-ISAC is a program within CIS.

Can the Center for Internet Security's MS-ISAC help me with a cyber incident?
Yes. CIS' Computer Emergency Response Team (CIS CERT) comprises highly trained staff who are able to assist you with a cybersecurity incident. CIS CERT can provide malware analysis, reverse engineering, log analysis, forensics analysis and vulnerability assessments. The Incident Response service is available to all SLTT entities – MS-ISAC membership is not required. If you are an SLTT entity and experience a cybersecurity incident or want to report an incident to improve situational awareness, contact us for assistance: soc@msisac.org or 1-866-787-4722.

Can other members of my organization join?
Yes. Each organization designates a "Primary Member" who is then responsible for authorizing additional individuals in their organization to become members.

Are there any requirements to join?
The only requirement is the completion of a membership agreement, which sets forth the responsibilities of members to protect information that is shared.

Are there any educational or training resources available?
Yes. In addition to advisories and information bulletins regarding the latest cyber threats and vulnerabilities, the MS-ISAC provides a variety of educational, awareness, and training resources and opportunities.

Does MS-ISAC work with federal agencies, private sector groups, and the other ISACs?
Yes. The MS-ISAC works closely with federal partners at DHS, along with Federal Bureau of Investigation, U.S. Secret Service and others to better share information on emerging threats. The MS-ISAC also has strong relationships with major internet service providers, cyber security firms, researchers, and software developers.

How do I join?
Contact the CIS MS-ISAC at info@msisac.org or visit https://msisac.cisecurity.org to learn more.

Attachment C

CIS Critical Security Controls

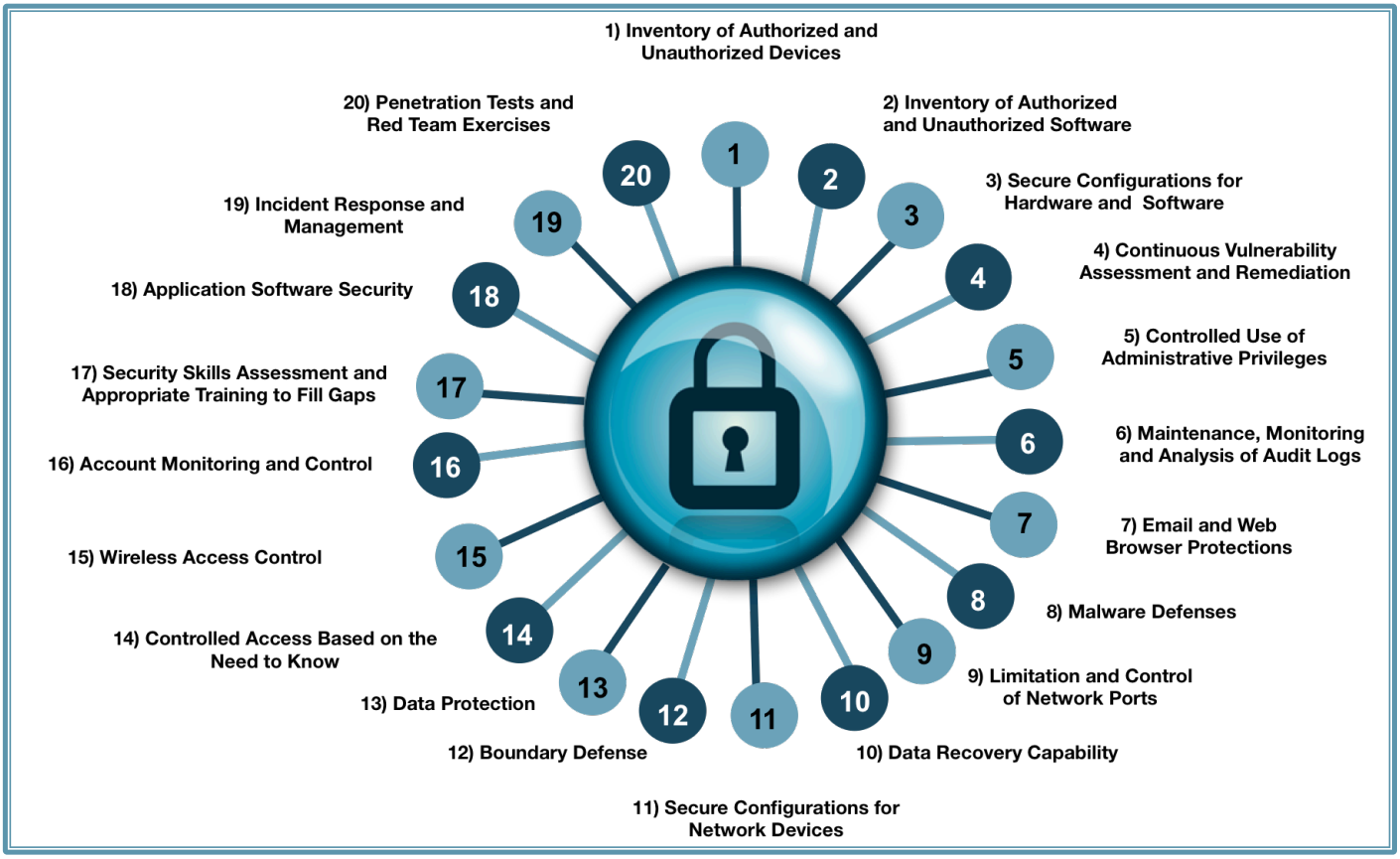
The **CIS Critical Security Controls**™ (CIS Controls) are a concise, prioritized set of cyber practices created to stop today's most pervasive and dangerous cyber attacks. The Controls are developed, refined, and validated by a community of leading experts from around the world.

Organizations that implement the CIS Controls can prevent the vast majority of cyber attacks.

Available as a free PDF download, the CIS Controls are written to address a smaller number of actions with a high payoff – a **"must do first"** philosophy – so implementing even a few of the CIS Controls can dramatically improve your network security posture.

The CIS Controls are:

- Regularly updated by cyber experts based on actual attack data pulled from a variety of public and private threat sources
- Supported by numerous security solution vendors, integrators, and consultants
- Referenced by the U.S. Federal Government in the NIST Cybersecurity Framework and other guidelines, and validated by the Australian government
- Recommended by the U.S. National Governor's Association, the UK's Centre for the Protection of National Infrastructure (*CPNI*), Symantec, Zurich Insurance, and others



Download the CIS Controls at https://www.cisecurity.org/critical-controls.cfm

Attachment D

CIS SECURITY BENCHMARKS RESOURCES

Over 100 Benchmarks Covering 14 Technology Groups

DOWNLOAD FREE PDFS – https://benchmarks.cisecurity.org/downloads

- **Authentication Servers**
  - Free RADIUS
  - MIT Kerberos
- **Cloud Providers**
  - Amazon Web Services
- **Database Platforms**
  - IBM DB2 Server
  - Microsoft SQL Server
  - MySQL Database Server
  - Oracle Database Server
- **Directory Servers**
  - Novell eDirectory
  - OpenLDAP Server
- **DNS Servers**
  - Bind DNS Server
- **Mail Servers**
  - Microsoft Exchange
- **Mobile Platforms**
  - Apple Mobile Platform
  - Google Mobile Platform
- **Network Devices**
  - Checkpoint Firewall
  - Cisco Firewall Devices
  - Cisco Routers/Switches
  - Juniper Routers/Switches
  - Agnostic Print Devices
  - Agnostic Wireless Devices
- **Operating Systems: Desktop**
  - Apple Desktop
  - Microsoft Windows
- **Operating Systems: Servers**
  - Amazon Linux
  - CentOS
  - Debian Linux Server
  - Distribution Independent Linux
  - FreeBSD Server
  - HP-UX Server
  - IBM AIX Server
  - Microsoft Windows Server
  - Novell Netware
  - Oracle Linux
  - Oracle Solaris Server
  - Red Hat Linux Server
  - Slackware Linux Server
  - SUSE Linux Server
  - Ubuntu LTS Server
- **Productivity Software**
  - Microsoft Office
- **Virtualization Platforms**
  - VMware Server
  - Xen Server
  - Agnostic VM Server
- **Web Browsers**
  - Google Chrome
  - Microsoft Internet Explorer
  - Mozilla Firefox Browser
  - Opera Browser
- **Web Servers**
  - Apache HTTP Server
  - Apache Tomcat Server
  - Microsoft IIS Server
  - Apple Safari Browser

Resource Links

CIS Configuration Assessment Tool & Trial Information:
https://benchmarks.cisecurity.org/tools

Remediation Content:
https://benchmarks.cisecurity.org/downloads/remediation-content

Hardened Virtual Images:
https://benchmarks.cisecurity.org/hardened-virtual-images

For more information on the CIS resources and membership opportunities, please contact us at members@cisecurity.org

Center for Internet Security • 31 Tech Valley Drive
East Greenbush, NY 12061 • 518-266-3460

Member Only Resources

https://benchmarks.cisecurity.org/membership

CIS Configuration Assessment Tool (CIS-CAT)

- Quickly identify system security issues
- Routinely assess the configuration of production systems compared to over 80 CIS Benchmarks and internal security policies
- Dashboard provides visual overall, device, or technology group of benchmark performance over time
- Vulnerability Assessment (Windows, RHEL, SUSE)
- SCAP Validated as an Authenticated Configuration Scanner - SCAP 1.2 Compliant

Remediation Content – Quickly implement CIS security recommendations using CIS's automated remediation content.

- Amazon Linux 2014.09-2015.03
- Microsoft Windows 7, 8, 8.1 & 10
- Microsoft Windows Server 2003, 2008, 2008 R2, 2012 & 2012 R2
- Microsoft Windows XP
- Microsoft Outlook 2010
- Microsoft Office 2013 & 2016, Access 2013 & 2016, Excel 2013, Outlook 2013 & 2016, Word 2013 & 2016, PowerPoint 2013 & 2016
- Microsoft Internet Explorer 9, 10 & 11
- IBM AIX 5.3-6.1 & 7.1
- Red Hat Enterprise Linux 6 & 7
- Oracle Linux 7
- CentOS Linux 6 & 7
- HP-UX
- SUSE Linux Enterprise Server 11 & 12
- Google Chrome 49
- Mozilla Firefox 38 ESR
- Debian 7 & 8

CIS-Hardened Virtual Images – Configured according to CIS Security Benchmarks in the Amazon Web Services Elastic Compute Cloud.

- Amazon Linux 2014.09 -2015.03
- Debian 8
- Microsoft Windows Server 2008 R2 & 2012 R2
- Red Hat Enterprise Linux 5, 6 & 7
- SUSE Linux Enterprise Server 11 & 12
- CentOS Linux 6 & 7
- Ubuntu 12.04 & 14.04 LTS Server

5/16

CIS CONFIGURATION ASSESSMENT TOOL (CIS-CAT)

Description

CIS-CAT is a configuration assessment/audit software tool available to CIS Security Benchmarks Members. Written in Java, CIS-CAT: (a) reads those CIS Security Benchmarks that are expressed in XCCDF (XML) format; (b) reports the configuration status of a target system as compared to the technical controls defined in those CIS Benchmarks; (c) provides a comparative score based on a conformity scale of 0-100; and (d) features Report Aggregation (a CIS-CAT Dashboard).

CIS-CAT is SCAP Validated as an Authenticated Configuration Scanner! For more information, visit http://nvd.nist.gov/scap/validation/127.cfm and the CIS-CAT User's Guide.

CIS-CAT consumes XML representations of various CIS Benchmarks. The XML schemas used to express CIS benchmarks are XCCDF, OVAL, and ECL. The XCCDF schema is used to describe and group configuration states while OVAL and ECL are used to define how to test a system's conformance with the configuration state described in XCCDF. All CIS Benchmarks that are expressed in XML are expressed in XCCDF+ECL and/or XCCDF+OVAL. Vulnerability assessment capabilities available for Microsoft Windows Desktops and Servers, SUSE and Red Hat Enterprise Linux.

For information on OVAL, visit http://oval.mitre.org/, or on XCCDF, visit http://scap.nist.gov/specifications/xccdf/.

System Requirements

CIS-CAT requires JRE v1.6 or later. The tool and the JRE can reside on the target system of evaluation, a removable or network drive, provided it is accessible from the target of evaluation. Distributed in both CLI and GUI versions, CIS-CAT is a host based scanning tool. CIS provides supplemental scripts that support CIS-CAT in assessing multiple systems simultaneously. CIS-CAT is not a network or enterprise scanner and does not change configuration settings.

Platform Support

CIS-CAT can read customized input files and compare the configuration of systems to both the CIS benchmarks and customized configuration policies. This feature is enabled by user modification of the Benchmark XCCDF files.

CIS-CAT reads: (a) Over 80 CIS Benchmarks currently available in XCCDF); (b) XCCDF configuration files distributed by NIST for Microsoft Win XP and Vista, and (c) user-modified CIS Benchmark XCCDF files. Benchmark coverage (* denotes OVAL coverage):

- Amazon Linux 2014.09-2015.03*
- Apache Tomcat 5.5-6.0
- Apple OSX 10.5, 10.6, 10.8, 10.9, 10.10, 10.11
- Cisco IOS 12*, 15 *
- CentOS Linux 6 *& 7*
- Debian Linux 3, 7* & 8*
- Google Chrome 46*
- HP-UX 11i
- IBM AIX 4.3-5.1, 5.3-6.1, 7.1
- Microsoft Internet Explorer 10* & 11*
- Microsoft IIS 7/7.5* & 8/8.5*
- Microsoft Office 2013* & 2016*
- Microsoft Access 2013* & 2016*
- Microsoft Outlook 2013* & 2016*
- Microsoft Powerpoint 2013* & 2016*
- Microsoft Word 2013* & 2016*
- Microsoft Excel 2013* & 2016*
- Microsoft SQL Server 2008 R2*, 2012*, 2014*
- Microsoft Windows XP*, 7*, 8, 8.1*, 10*
- Microsoft Windows 2003 MS DC*, 2008 Server*, 2008 R2 Server*, 2012 Server*, 2012 R2 Server*
- MIT Kerberos KDC 1.10*
- Mozilla Firefox 3, ESR 24*, ESR 38*
- Oracle Database 9i-10g , 11g , 11g R2*, 12c
- Oracle Linux 7*
- Oracle MySQL Community Server 5.6* & 5.7*
- Oracle MySQL Enterprise Edition 5.6* & 5.7*
- Oracle Solaris 2.5.1-9, 10, 11, 11.1, 11.2
- Red Hat Enterprise Linux 4, 5*, 6*, 7*
- Slackware Linux 10.2
- SUSE Linux Enterprise Server 9, 10, 11*, 12*
- Ubuntu 12.04 LTS Server & 14.04 LTS Server

Download Files & User Support

Members can download the CIS-CAT bundle from the community site downloads.
Additional guidance and support is provided to members via the member discussions, tutorials and support by CIS staff.
To learn more about membership or obtain a trial use of the CIS-CAT Tool contact us at members@cisecurity.org.

5/16

Center for Internet Security

Steven J. Spano
Brigadier General, USAF (Ret.)
President & Chief Operating Officer
Center for Internet Security

Brigadier General (retired) Steve Spano is President and Chief Operating Officer of the Center for Internet Security (CIS). Prior to joining CIS in May 2015, he served as the General Manager, Defense and National Security, for Amazon Web Service's (AWS) Worldwide Public Sector. General Spano was one of the key leaders who helped launch and build the public sector business from its inception in 2011. He also led the sales effort to close the biggest deal in AWS history – a private cloud region for the United States intelligence community.

Prior to Amazon Web Services, he served more than 28 years in the United States Air Force as an IT professional, serving in numerous command, staff, and CIO leadership roles. His numerous awards and decorations include the Defense Superior Service Medal, Legion of Merit, and Bronze Star.

General Spano earned a Bachelor of Science in Business Administration from Norwich University; a Master of Administrative Science in Management from Johns Hopkins University; and a Master of Science in Strategic Studies from Air War College.