



Cybersecurity for the Therapy Provider

Finding a Practical Balance Between Security and Productivity

Michael Duncan – Strategic Account Executive – Healthcare

Matthew McGarvey – Strategic Account Executive – Healthcare

March 13, 2025

Internal Only - General

Confidential & Proprietary

1



Housekeeping Items

- This webinar is being recorded and will be available on NARA's general website and Member portal on Monday, March 17.
 - NARA Website: www.naranet.org > Resources > Quicklinks
- Questions for Speakers:
 - Please use the Q&A button located on your attendee toolbar
- General/Technical Questions:
 - Please use the Chat button located on your attendee toolbar



Confidential & Proprietary

Internal Only - General

2



Today's Presenters

Mike Duncan and Matt McGarvey – CIS Strategic Healthcare Team



Confidential & Proprietary

Internal Only - General

3



About CIS

The Center for Internet Security



Independent and Trusted



Proven and Effective



Collaborative



Operational Expertise



Sustainable

Confidential & Proprietary

Internal Only - General

4



Mission and Vision

Mission

- Make the connected world a safer place by developing, validating, and promoting timely best practice solutions that help people, businesses, and governments protect themselves against pervasive cyber threats.

Vision

- Leading the global community to secure our ever-changing connected world.

*Creating Confidence in
the Connected World™*

Confidential & Proprietary

Internal Only - General

5



Healthcare Safeguard Patient Data

Strengthen your Security
Ensuring Continuity of Care
in a Connected World



**Empower Patient Care with
the latest in Cybersecurity**

Confidential & Proprietary

Internal Only - General

6



Cybersecurity & Healthcare

- **US Healthcare is currently ~18% of total GDP**
 - Federally designated as U.S. Critical Infrastructure
- **The healthcare industry has become a prime target for Hackers**
 - Healthcare has traditionally under-invested in cybersecurity protections
 - From 2018 to 2022, HHS tracked a 95% increase in large data breaches / ransomware attacks.
 - Understaffed and overwhelmed IT and information security departments
- **The sector could still be moving toward mandated cybersecurity protections**
 - Legislation would have allowed emergency payments in case of an attack but only if covered entities meet a minimum level of cyber security protections.

Confidential & Proprietary

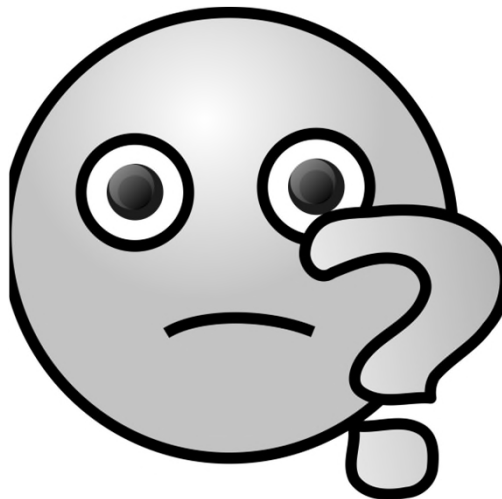
Internal Only - General

7



Government Response

Legislation, Guidelines, Regulations, Executive Action



Are Federal
Cybersecurity
Regulations
Coming?

Confidential & Proprietary

Internal Only - General

8



Government Response

Legislation, Guidelines, Regulations, Executive Action

- Bills were introduced in 2023 and 2024 around healthcare cybersecurity regulations. These appear to be dead.
- New bills could be introduced in 2025
- The “Proposed Rule” Phase for HIPPA 2.0 just ended last week. In addition to many updates involving PHI, security and incident response were introduced
 - **Security:** Covered entities must implement security measures like encryption, multi-factor authentication, and vulnerability scanning.
 - **Incident response:** Covered entities must establish written procedures for responding to security incidents.
- **“As of Right Now”** we can’t officially speculate the outcome as it is difficult to predict.

Confidential & Proprietary

Internal Only - General

9



Healthcare

Challenges in Healthcare Cybersecurity Take on Many Forms



Continuity of Operations not just Data Protection.



Elevated Third-Party Risk



Acquisition and Consolidation Risks



Very High Stakes



Highly Complex I.T. Infrastructure

Confidential & Proprietary

Internal Only - General

10



As an Industry, What Historically Drives Change in Healthcare

In no particular order

- Response to Regulatory Requirements and Legislation
- Revenue Increase or Cost / Time Savings
- Improve Patient Care



Confidential & Proprietary

Internal Only - General

11



Elevated Third-Party Risk



- **Healthcare relies on a concentrated number of service providers to maintain financial health i.e. Rev Cycle Services**
- **Multiple provider organizations must share data and systems in order to maintain continuity of care**
- **Risk associated with not fully understanding the impact of losing third-party services i.e. Change HC**

Confidential & Proprietary

Internal Only - General

12



Acquisition and Consolidation



- **Aggressive and dynamic acquisition strategies leave operators with little time and minimal resources to conduct due diligence**
- **Healthcare systems must contend with 'weakest link' issues when making new acquisitions**
- **Organizational and operational upheaval creates additional risk**

Confidential & Proprietary

Internal Only - General

13



Continuity of Operations



- **Connected Medical Devices such as therapy equipment, insulin pumps, ventilators, blood pressure monitors, etc. make up most of a providers end points. They cannot go down.**
- **'Operating on Paper' is no longer an option**
- **Critical Systems (EHR, ER, Inpatient, MedRec) must remain operational or patient care and safety will be impacted**

Confidential & Proprietary

Internal Only - General

14



High Stakes



- **Every decision must take operational, financial and patient safety issues into consideration**
- **Patient safety comes first**
- **Rural healthcare providers have even less resources to serve their communities**
- **Cybercriminals know this and expect to get the ransom more easily**

Confidential & Proprietary

Internal Only - General

15



Complex I.T. Infrastructure



- **Few industries leverage as much different / proprietary technology in their environment as healthcare - i.e. server, device, desktop, virtual, software, embedded, cloud services etc..**
- **End users go outside of protected networks in the interest of expediency (i.e. using yahoo account to send info because it is faster)**
- **Domain expertise to understand the vulnerabilities of each technology is extremely difficult to find**

Confidential & Proprietary

Internal Only - General

16



Artificial Intelligence in Healthcare

- **Many different types of AI (common examples include)**
 - Machine Learning
 - Generative
 - Agent Based
- **Our recommendation is to establish a company policy for adherence**
- **Ensure that you are using the CIS Critical Security Controls as part of your vetting process for any AI tool**

Confidential & Proprietary

Internal Only - General

17



Cybersecurity for the Therapist

Finding the Security and Productivity Balance

Confidential & Proprietary

Internal Only - General

18



Special Challenges Faced by Therapy Providers

- **Pressure to complete treatments, meet a productivity threshold, and perform documentation ON TIME!**
- **With electronic documentation systems being used, uninterrupted connectivity is a must**
- **Are those connections always secure?**
- **Even if they are secure, there is still vulnerability**

Confidential & Proprietary

Internal Only - General

19



What Happens When There is a Problem?

Uh Oh, my system doesn't work



I always just called the guy!!!

Confidential & Proprietary

Internal Only - General

20



Special Challenges Faced by Therapy Providers

- **Any interruption causes your day to quickly fall off track disrupting:**
 - Operations
 - Patient Care
 - Your Productivity
 - Billing
 - Everyone Else's Day
- **How do I know if it is a security breach, or just a routine problem for the guy to fix?**

Confidential & Proprietary

Internal Only - General

21



How Do I Identify a Security Breach?

Methods of Being Vigilant



Wait a minute.... I am a therapist.

I didn't know it was my job to identify a security breach!

Confidential & Proprietary

This Photo by Unknown Author is licensed under [CC BY](#)

Internal Only - General

22



How Can My Organization Protect Itself from Cyberthreat?

- How can my organization strike that balance between security and allowing the clinicians do perform patient care?
- What can I do, within my role, to help?
- How do we establish a security culture for the good of the organization and the patients?
- What is a reasonable amount of staff education?
- Where do we even begin?

Confidential & Proprietary

Internal Only - General

23



Most Common Types of Cyberthreats

(In Everyday Language)

- Let's Begin by Learning the Most Common Types of Cyberthreats so We Can All Be Vigilant



Confidential & Proprietary

Internal Only - General

24



Identifying the 5 Most Common Types of Attacks

- **Malware – Intrusive software installed by cybercriminals on your computer to damage and destroy your systems**
- **Ransomware – A type of malicious software designed to block access to a computer system until a sum of money is paid**
- **Web Application Hacking – When cybercriminals “break in” to web-based systems to collect sensitive data & use that to get access to your network**

Confidential & Proprietary

Internal Only - General

25



Identifying the 5 Most Common Types of Attacks

- **Insider Privilege and Misuse – Inappropriate or fraudulent use of privileges associated with a user’s account**
- **Targeted Intrusions - Calculated efforts by threat actors to infiltrate systems, steal sensitive data, and disrupt critical operation**

Confidential & Proprietary

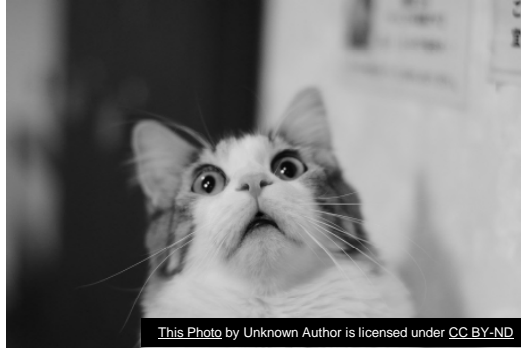
Internal Only - General

26



What Do We Do Now That We Are Scared?

Protect the Organization and the Patients



- **Now that we are all scared, what do we do so we aren't either broke or out of business... or both!**

Confidential & Proprietary

Internal Only - General

27



Adopt an Organizational Approach

Develop a Plan

- **Establish an organizational approach to security**
- **As an organization, begin by defining what is a reasonable standard of cybersecurity for you**



Confidential & Proprietary

Internal Only - General

28



CIS Critical Security Controls®

Prescriptive Guidance to Protect Against Cyber Crime

Internal Only - General

Confidential & Proprietary



CIS Critical Security Controls® Version 8.1

18 top-level best practices containing 153 prioritized safeguards

CONTROL 01	Inventory and Control of Enterprise Assets	CONTROL 02	Inventory and Control of Software Assets	CONTROL 03	Data Protection
CONTROL 04	Secure Configuration of Enterprise Assets and Software	CONTROL 05	Account Management	CONTROL 06	Access Control Management
CONTROL 07	Continuous Vulnerability Management	CONTROL 08	Audit Log Management	CONTROL 09	Email and Web Browser Protections
CONTROL 10	Malware Defenses	CONTROL 11	Data Recovery	CONTROL 12	Network Infrastructure Management
CONTROL 13	Network Monitoring and Defense	CONTROL 14	Security Awareness and Skills Training	CONTROL 15	Service Provider Management
CONTROL 16	Applications Software Security	CONTROL 17	Incident Response Management	CONTROL 18	Penetration Testing

Internal Only - General

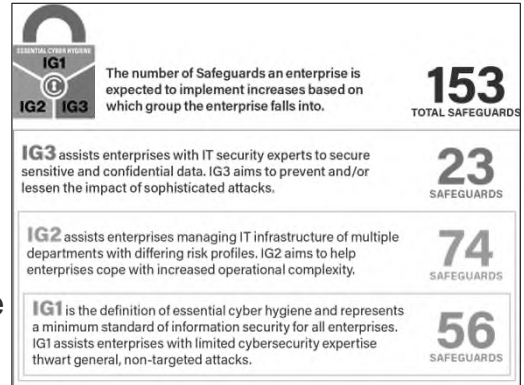
Confidential & Proprietary



CIS Controls®

Prescriptive, prioritized, and simplified set of cybersecurity best practices

- **Implementation Group 1**
 - Every organization starts here – definition of essential cyber hygiene
- **Implementation Group 2**
 - Moderate resources and expertise
- **Implementation Group 3**
 - Significant resources and expertise



Confidential & Proprietary

Internal Only - General

31



CIS CDM v2.0 Summary

Top 5 Attacks	IG1 CIS Safeguards IG1 can defend against XX% of ATT&CK (Sub-)Techniques	All CIS Safeguards CIS Safeguards can defend against XX% of ATT&CK (Sub-)Techniques
Malware	77%	94%
Ransomware	78%	92%
Web Application Hacking	86%	98%
Insider Privilege and Misuse	86%	90%
Targeted Intrusions	83%	95%

All percentages are based on ATT&CK (sub-)techniques assigned to an ATT&CK mitigation.

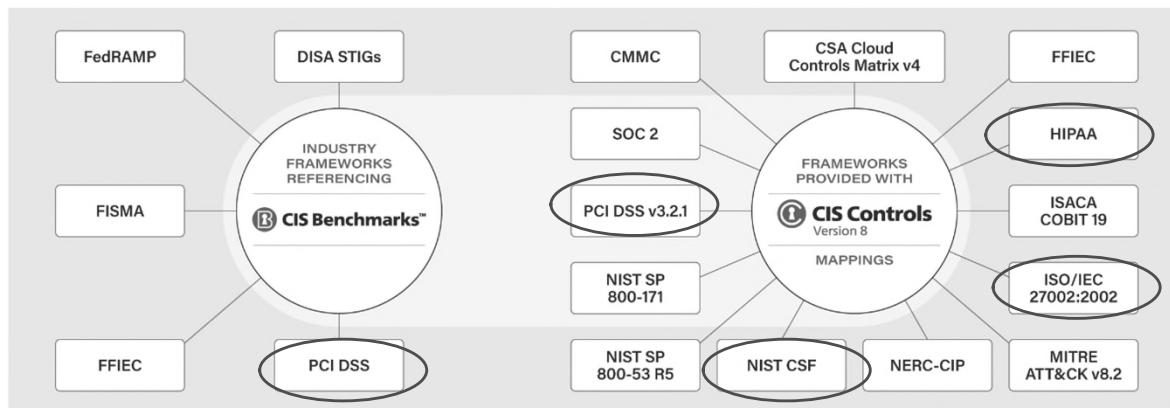
Internal Only - General

32

CIS. Continuity of Operations



Referenced by Industry Standards



Confidential & Proprietary

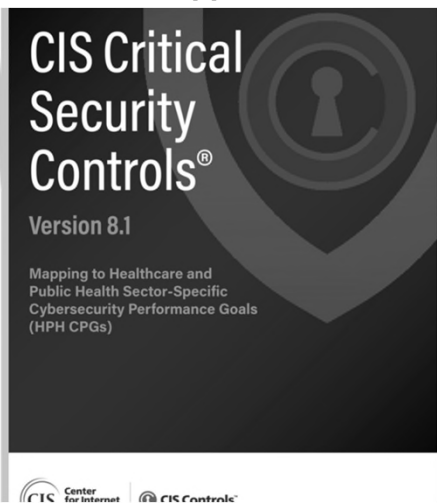
Internal Only - General

33

CIS. The HPH CPG Framework



Now Mapped to the HPH CPGs!




CIS Control ID	Asset Type	Priority	Title	Description	Relationship	Goal	Description
6.13	User	Protect	Require MFA for Remotely Executed Applications	Require MFA for all remote access to critical systems, including remote desktop, VPN, and other remote access methods. MFA should be implemented for all remote access to critical systems, including remote desktop, VPN, and other remote access methods. MFA should be implemented for all remote access to critical systems, including remote desktop, VPN, and other remote access methods.	Subpart	Multifactor Authentication	Add a critical, additional layer of security, when used with the baseline controls, to protect accounts and accounts directly accessible from the Internet.
6.14	User	Protect	Require MFA for Remote Network Access	Require MFA for all remote network access to critical systems, including remote desktop, VPN, and other remote access methods. MFA should be implemented for all remote network access to critical systems, including remote desktop, VPN, and other remote access methods.	Subpart	Multifactor Authentication	Add a critical, additional layer of security, when used with the baseline controls, to protect accounts and accounts directly accessible from the Internet.
6.15	User	Protect	Require MFA for Administrative Access	Require MFA for all administrative access to critical systems, including remote desktop, VPN, and other remote access methods. MFA should be implemented for all administrative access to critical systems, including remote desktop, VPN, and other remote access methods.	Subpart	Multifactor Authentication	Add a critical, additional layer of security, when used with the baseline controls, to protect accounts and accounts directly accessible from the Internet.
6.18	Software	Identify	Establish and Maintain an Inventory of Administrative and Privileged Accounts	Establish and maintain an inventory of all administrative and privileged accounts used for system management. The inventory should include account names, roles, and access permissions. The inventory should be updated regularly and used to manage account lifecycle.			

CIS Control ID	Asset Type	Priority	Title	Description	Relationship	Goal	Description
7.11	Documentation	Identify	Establish and Maintain a Vulnerability Management Process	Establish and maintain a vulnerability management process that includes regular scanning for vulnerabilities, prioritization of findings, and remediation. The process should include regular scanning for vulnerabilities, prioritization of findings, and remediation. The process should include regular scanning for vulnerabilities, prioritization of findings, and remediation.	Subpart	Mitigate Known Vulnerabilities	Reduce the likelihood of threat actors exploiting known vulnerabilities to breach organizational networks that are directly accessible from the Internet.
7.12	Documentation	Identify	Establish and Maintain a Configuration Management Process	Establish and maintain a configuration management process that includes regular updates, testing, and deployment of configurations. The process should include regular updates, testing, and deployment of configurations. The process should include regular updates, testing, and deployment of configurations.	Subpart	Mitigate Known Vulnerabilities	Reduce the likelihood of threat actors exploiting known vulnerabilities to breach organizational networks that are directly accessible from the Internet.
7.13	Software	Protect	Perform Automated Operating System Patch Management	Perform automated operating system patch management on all critical systems. The process should include regular updates, testing, and deployment of patches. The process should include regular updates, testing, and deployment of patches.			
7.14	Software	Protect	Perform Automated Application Patch Management	Perform automated application patch management on all critical systems. The process should include regular updates, testing, and deployment of patches. The process should include regular updates, testing, and deployment of patches.			

Confidential & Proprietary

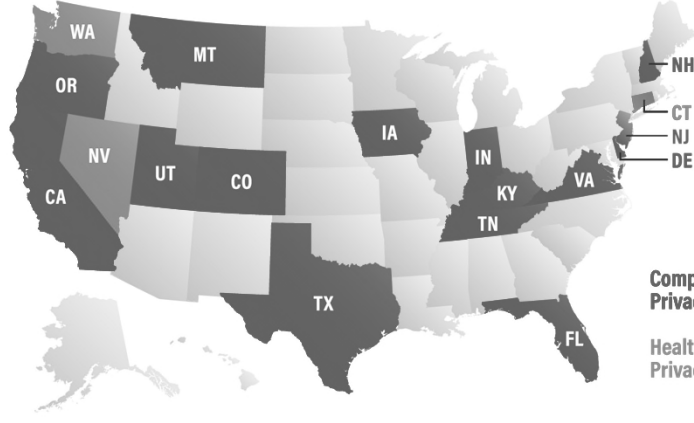
Internal Only - General

34



State Data Privacy Laws

Many States are Adopting Laws where a Security Framework like CIS is the Expectation




Comprehensive Data Privacy Statutes

Health Data Privacy Statutes






2020 2021 2022 2023 2024

Confidential & Proprietary
Internal Only - General

35

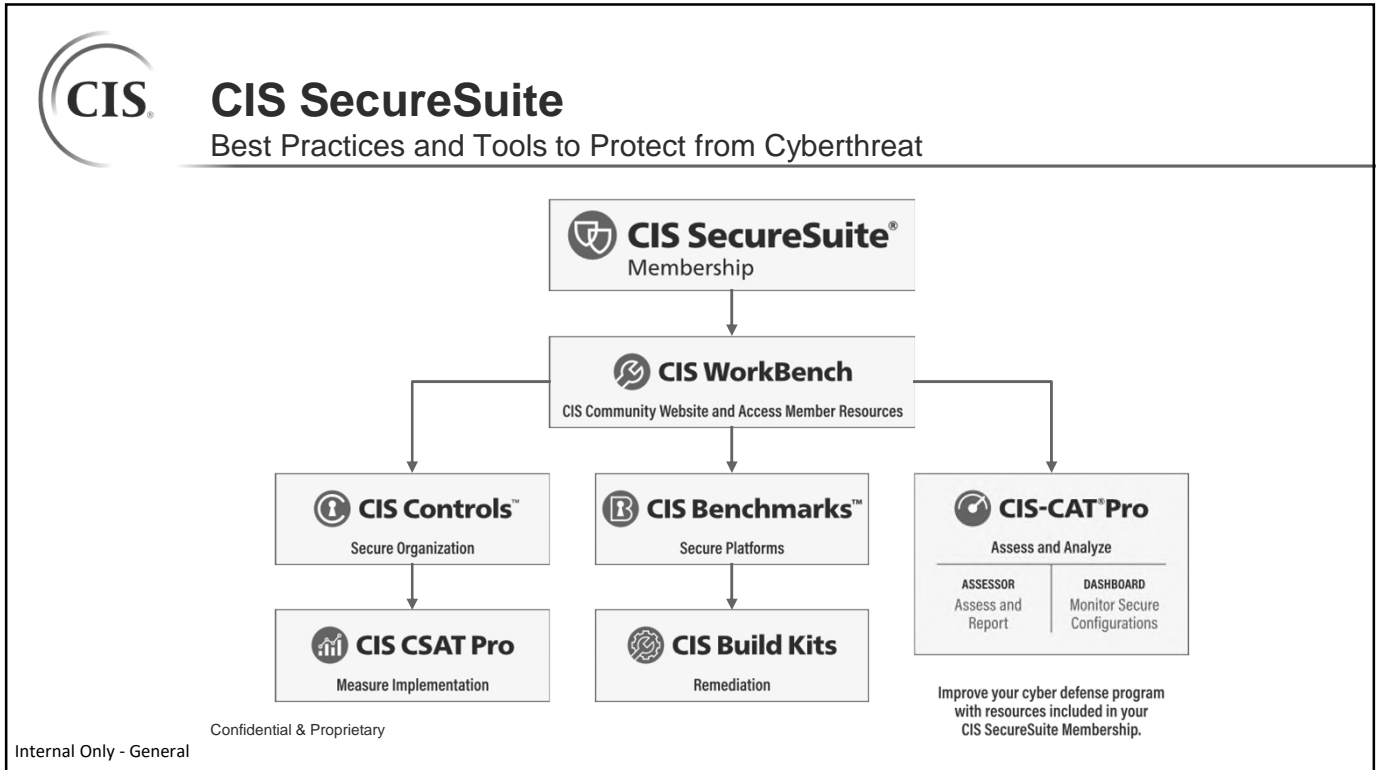


Solutions to Healthcare's Unique Problems

 <p>Continuity of Operations & Data Protection</p> <p>Reduce work of distilling dozens of compliance frameworks into actionable goals by using CIS Controls and CIS Benchmarks</p> <p>Confidential & Proprietary</p>	 <p>Elevated Third Party Risks</p> <p>Leverage the resources specific to CIS Controls</p>	 <p>Acquisition and Consolidation</p> <p>Use the CIS Controls as a prescriptive guide to increase effectiveness and reduce due diligence timeframes</p>	 <p>High Stakes</p> <p>Use the CIS Controls to Educate staff on cybersecurity best practices to help reduce the risk of human error</p>	 <p>Complex IT Infrastructure</p> <p>Identify and address with CIS Benchmarks misconfigurations in your IT infrastructure and connected medical devices to minimize your attack surface</p>
--	---	---	--	---

Confidential & Proprietary
Internal Only - General

36



37

-
- CIS SecureSuite Tools**
- CIS Controls
 - CIS Benchmarks
 - CIS-CSAT Pro
 - CIS-CAT Pro Assessor
 - CIS-CAT Pro Dashboard
 - CIS RAM
 - CIS Workbench
- Confidential & Proprietary
- Internal Only - General

38



CIS SecureSuite Membership Types

- **End Users**
 - Organizations using the Membership resources to harden internal systems and data.
- **Services and Consulting**
 - Organizations and individual consultants who leverage the CIS SecureSuite resources to help clients enhance their cybersecurity.
- **Product Vendors**
 - Organizations who typically import the CIS Benchmarks into another tool or product offering. Certifications available with Membership.

Confidential & Proprietary

Internal Only - General

39



Discount Exclusively for NARA Members

Up to **20% off** on CIS SecureSuite through December 31, 2025!

Thank you for attending our special webinar. As a token of our appreciation, we'd like to offer webinar attendees this special discount.

Please use **promo code NARA25** to receive the exclusive discount.

Promo terms: <https://www.cisecurity.org/cis-securesuite/promo-terms>



CIS SecureSuite[®]

Start Secure. Stay Secure.[®]

Confidential & Proprietary

Internal Only - General

40



Questions, Demo Requests, More Info

Up to **20% off** on CIS SecureSuite through December 31, 2025!

Email: Matthew.McGarvey@cisecurity.org or
Michael.Duncan@cisecurity.org



CIS SecureSuite[®]

Start Secure. Stay Secure.[®]

Confidential & Proprietary

Internal Only - General

41



NARA Spring Regulatory & Legislative Conference

April 29 – May 2 – Washington DC

- **April 29: ½ day session on AI & Healthcare (separate registration required)**
- **April 30 – May 2: 3-day regulatory and legislative updates including Hill Visits on May 1 (scheduled for registered attendees by NARA)**

For more information visit: www.naranet.org/education

Confidential & Proprietary

Internal Only - General

42



Thank You!

We are here to be a resource to
NARA & the membership

Internal Only - General

Confidential & Proprietary