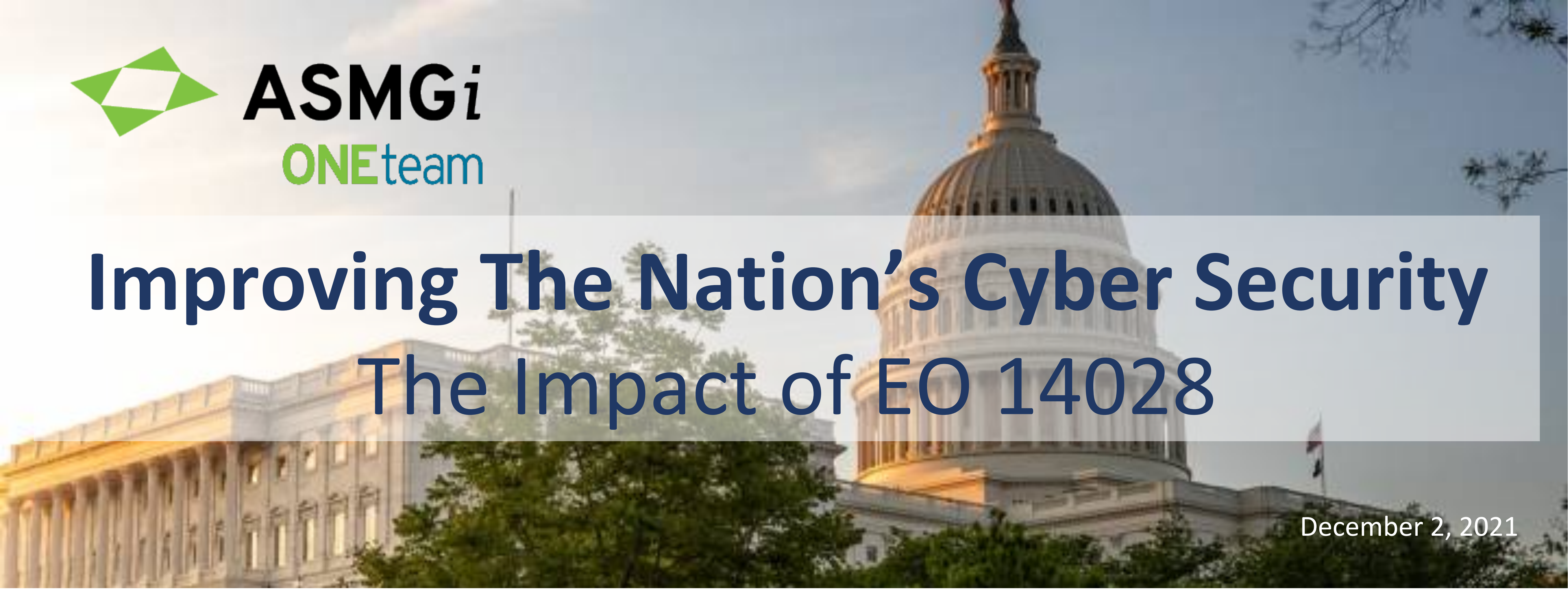


ASMGi ONEteam

Improving The Nation’s Cyber Security

The Impact of EO 14028

December 2, 2021

Cleveland Clinic

Rockwell Automation

EO 14028 – Improving The Nation's Cyber Security

Kevin Tambascio
IT/OT Attack Surface Reduction
Cleveland Clinic

Steve Roesing
President, CEO
ASMGi

Tony Baker
Chief Product Safety & Security Officer
Rockwell Automation

Executive Order 14028: Vendor and End-User Perspectives

Tony Baker

Chief Product Safety and Security Officer

Rockwell Automation

Kevin Tambascio

Cybersecurity Manager, IT/OT Attack Surface Reduction

Cleveland Clinic

Quick Facts

Executive Order (EO) 14028, “Improving the Nation’s Cybersecurity”, issued on May 12, 2021

6x

Larger than the typical Executive Order

70+

Actionable directives

40+

Defined deadlines

The term “Operational Technology”, or “OT”, is used throughout.

Areas of Focus

- Remove Barriers to Threat Information Sharing Between Government and the Private Sector.
- Modernize and Implement Stronger Cybersecurity Standards in the Federal Government
- Improve Software Supply Chain Security
- Establish a Cybersecurity Safety Review Board
- Create a Standard Playbook for Responding to Cyber Incidents
- Improve Detection of Cybersecurity Incidents on Federal Government Networks
- Improve Investigative and Remediation Capabilities

Themes

ASMGi ONEteam

Information Sharing

Remove contractual barriers and requires that all US government contracts ensure service providers collect and share cyber event details with US agencies.

Private → Government

Modernization

Significant emphasis on moving to the cloud, providing guidance on adoption and implementation, providing support for incident response, and how to engage with partners like CISA and FBI.

Zero Trust

Supply Chain

Objectives related to baseline security standards, vendors making security data public, incentivizing innovative approaches to securing software development, introduction of an “energy star” type of label.

Software Bill of Materials

(“SBOM”)

~30% of the directives in the EO are related to software supply chain security

Rockwell Automation

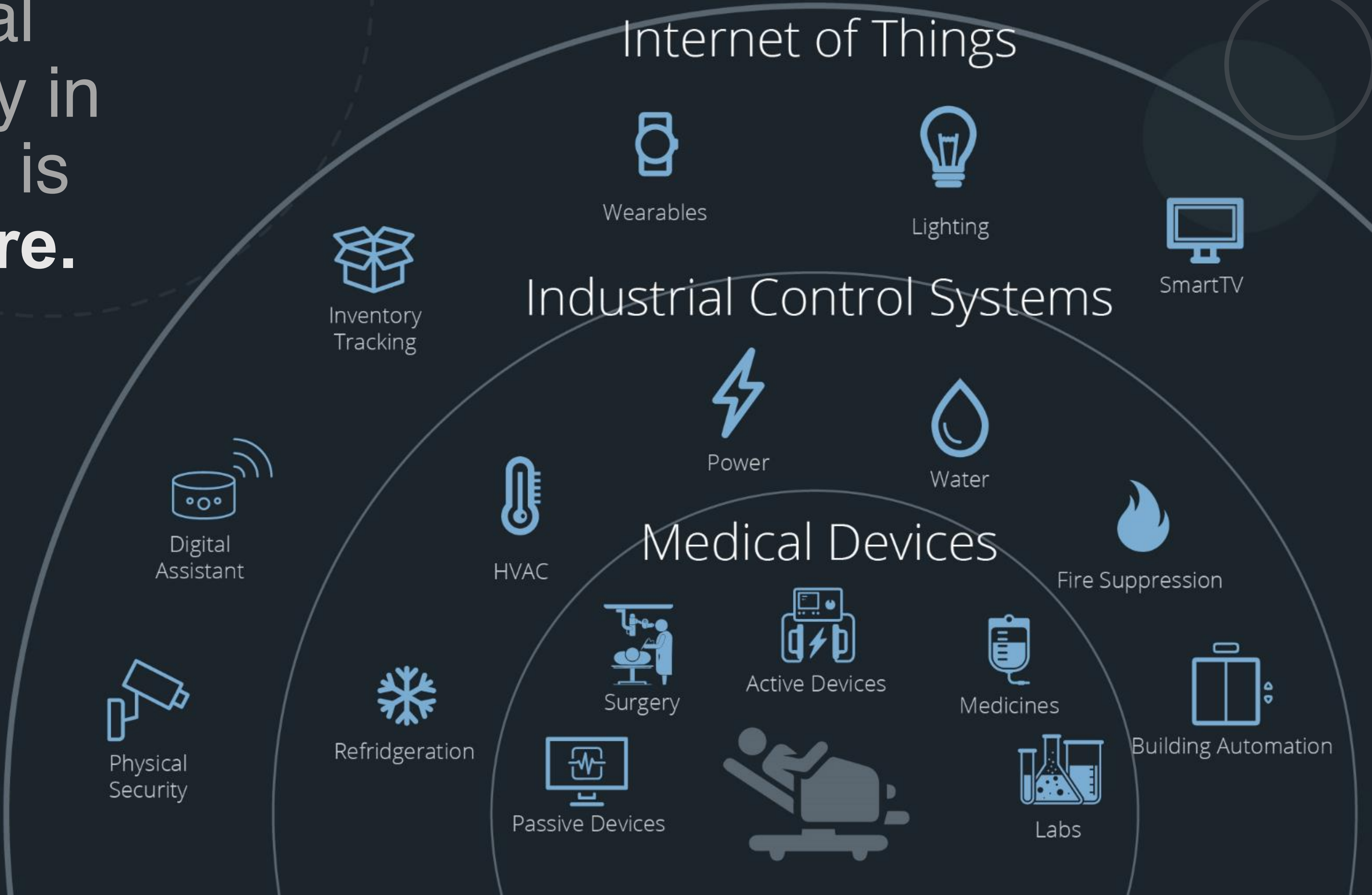
Vendor Impact

- Increased security information sharing with your customers
- Purposeful moving to “incentivize the market” leveraging “power of Federal procurement”
- Given the deadlines, expect changes to be swift
- (<7 months)

ASMGi ONEteam

Rockwell Automation

Operational Technology in healthcare is **everywhere.**



Internet of Things

Wearables

Lighting

SmartTV

Inventory Tracking

Digital Assistant

Physical Security

Industrial Control Systems

Power

Water

HVAC

Fire Suppression

Refridgeration

Building Automation

Medical Devices

Surgery

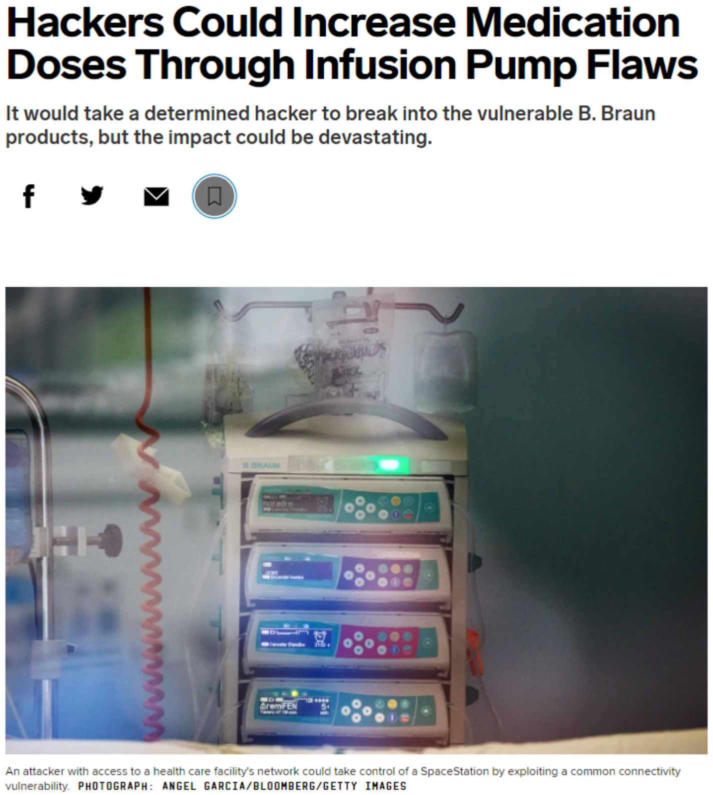
Active Devices

Medicines

Passive Devices

Labs

Cybersecurity Risks in Healthcare



Hackers Could Increase Medication Doses Through Infusion Pump Flaws

It would take a determined hacker to break into the vulnerable B. Braun products, but the impact could be devastating.

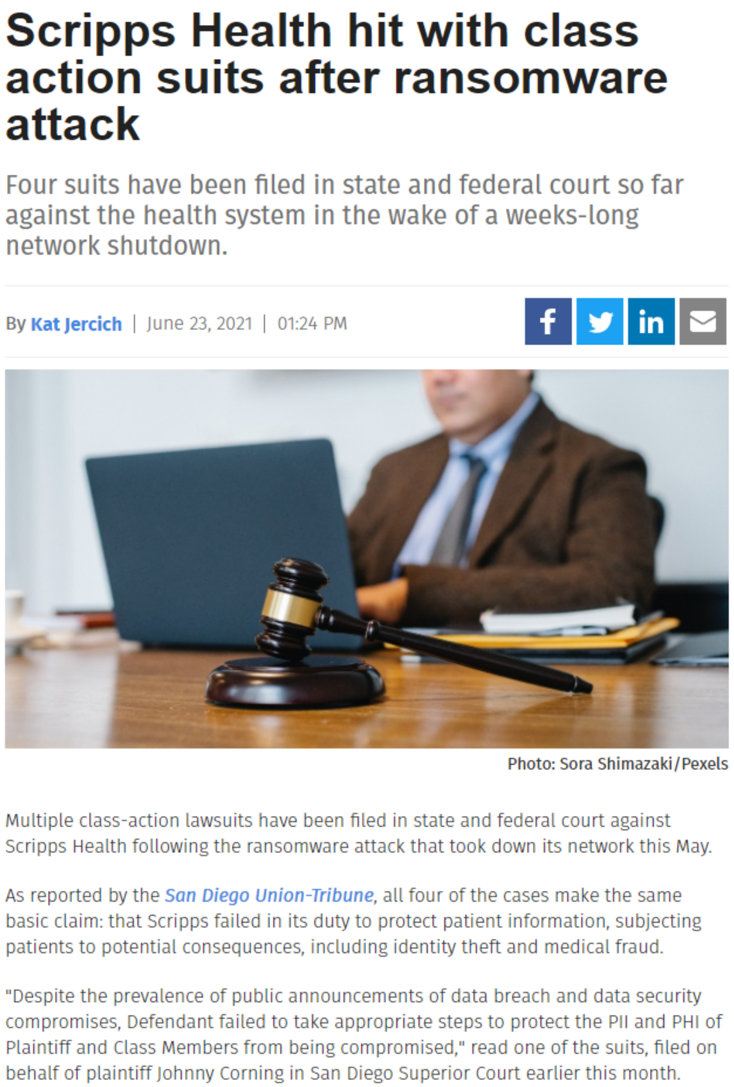
An attacker with access to a health care facility's network could take control of a SpaceStation by exploiting a common connectivity vulnerability. PHOTOGRAPH: ANGEL GARCIA/BLOOMBERG/GETTY IMAGES

Patient Safety

Availability of Care

Information Disclosure

Why Healthcare is Vulnerable to Ransomware



Scripps Health hit with class action suits after ransomware attack

Four suits have been filed in state and federal court so far against the health system in the wake of a weeks-long network shutdown.

By Kat Jercich | June 23, 2021 | 01:24 PM

Photo: Sora Shimazaki/Pexels

Multiple class-action lawsuits have been filed in state and federal court against Scripps Health following the ransomware attack that took down its network this May.

As reported by the *San Diego Union-Tribune*, all four of the cases make the same basic claim: that Scripps failed in its duty to protect patient information, subjecting patients to potential consequences, including identity theft and medical fraud.

"Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII and PHI of Plaintiff and Class Members from being compromised," read one of the suits, filed on behalf of plaintiff Johnny Corning in San Diego Superior Court earlier this month.

https://www.fiercehealthcare.com/tech/ransomware-attacks-cost-healthcare-industry-21b-2020-here-s-how-many-attacks-hit-providers

Cybersecurity Executive Orders – Key Takeaways

Enhancing Software Supply Chain Security

- Secure software development lifecycles
- Integrity of source code
- Software Bill of Materials
- Encryption of data
- Vulnerability Disclosure Programs
- Vulnerability assessments and cybersecurity testing

Joint Public/Private Partnerships

- Develop new approaches to securing critical software
- Information sharing on breaches and incidents
- Standardized incident response playbooks
- Standardized software rating system

Security Measures for “EO-Critical Software” Use

ASMGi
ONEteam

Objective 1: Protect EO-critical software and EO-critical software platforms from unauthorized access and usage.

Objective 2: Protect the confidentiality, integrity, and availability of data used by EO-critical software and EO-critical software platforms.

Objective 3: Identify and maintain EO-critical software platforms and the software deployed to those platforms to protect the EO-critical software from exploitation.

Objective 4: Quickly detect, respond to, and recover from threats and incidents involving EO-critical software and EO-critical software platforms.

Objective 5: Strengthen the understanding and performance of humans’ actions that foster the security of EO-critical software and EO-critical software platforms.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/security-measures-eo-critical-software-use

Cybersecurity Executive Orders – Will they reduce risk for ransomware?

Yes, Promising Start. Impact won’t be right away…

- VA is one the largest healthcare institutes and will impact medical vendors
- Enact change with a strong message to operators and vendors to improve

Basic Cybersecurity Hygiene Practices will reduce ransomware risk

- Improvements in vendors and products they sell
- Increased transparency enables risk analysis, controls, and incident response
- SBOM content will help drive vulnerability management practices
- Publicly available standards and playbooks help small-to-medium entities

HSCC Model Contract Language

- Includes many of the EO principles that we intend to use in our contract language

Who Is Responsible for Security – the Vendor or the Owner / Operator?

ASMGi
ONEteam

How Do You Identify Vulnerabilities in Products / Devices?   Who Fixes Them?

Q & A

Rockwell Automation

ASMGi

ONEteam

Patients

Caregivers

CARE

Community

Organization

100

YEARS

EST. 1921

Cleveland Clinic

Special Offers for Attendees

- ❑ Security Risk Ratings Report
  - ➢ ASMGi is offering a complimentary SecurityScorecard Detailed Security Ratings for your organization as well as up to three (3) third-party entities that are critical vendors for your organization as well as a session to review the information provided in the report.
- ❑ 50% Off a DevSecOps Maturity Assessment (includes information on creating an SBOM)

Contact sales@asmgi.com by Dec 17, 2021!

ASMGi

ONEteam

For more information:

800 Superior Ave E, Ste 1050
Cleveland, OH 44114

Phone: 216.255.3040
Email: sales@asmgi.com

www.asmgi.com