

# SUPPLY CHAIN ROCKS

## NEW BILLS AND REGULATIONS EMERGE



Recent and forthcoming regulation and government guidance regarding cybersecurity and supply chains globally have spurred a sense of urgency for organizations to invest in compliance.

A combination of proposed bills, executive orders, and standards are making their way through federal, state, and global forums to become the law of the land.

**We wish them well on their journey!**



## RECENTLY INTRODUCED SUPPLY CHAIN REGULATIONS & STANDARDS



### HOMELAND SECURITY CYBERSECURITY BILLS

Of 13 Homeland Security bills passed in July 2021, three focused on bolstering the cybersecurity of state and local government networks in response to ransomware and other cyber-attacks



### US EXECUTIVE ORDERS 14017

- Executive Order on America's Supply Chains
- Introduced by President Biden to increase resiliency in US supply chains, including mitigating foreign cyber-attacks



### GDPR DIRECTIVE ON SUPPLY CHAIN RISK

Building on GDPR's initial focus on data protection, recent expansion put accountability on companies to ensure that their full supply chain is GDPR compliant



### BIPARTISAN DATA PRIVACY BILL DRAFTED

Bipartisan bill drafted to reintroduce the Social Media Privacy Protection and Consumer Rights Act, forcing tech companies to grant users greater control over their data



### NIST 800-53 REV 5

- Security and Privacy Controls for Information Systems and Organizations
- Guidance for how organizations should select and maintain customized security and privacy controls for their information systems



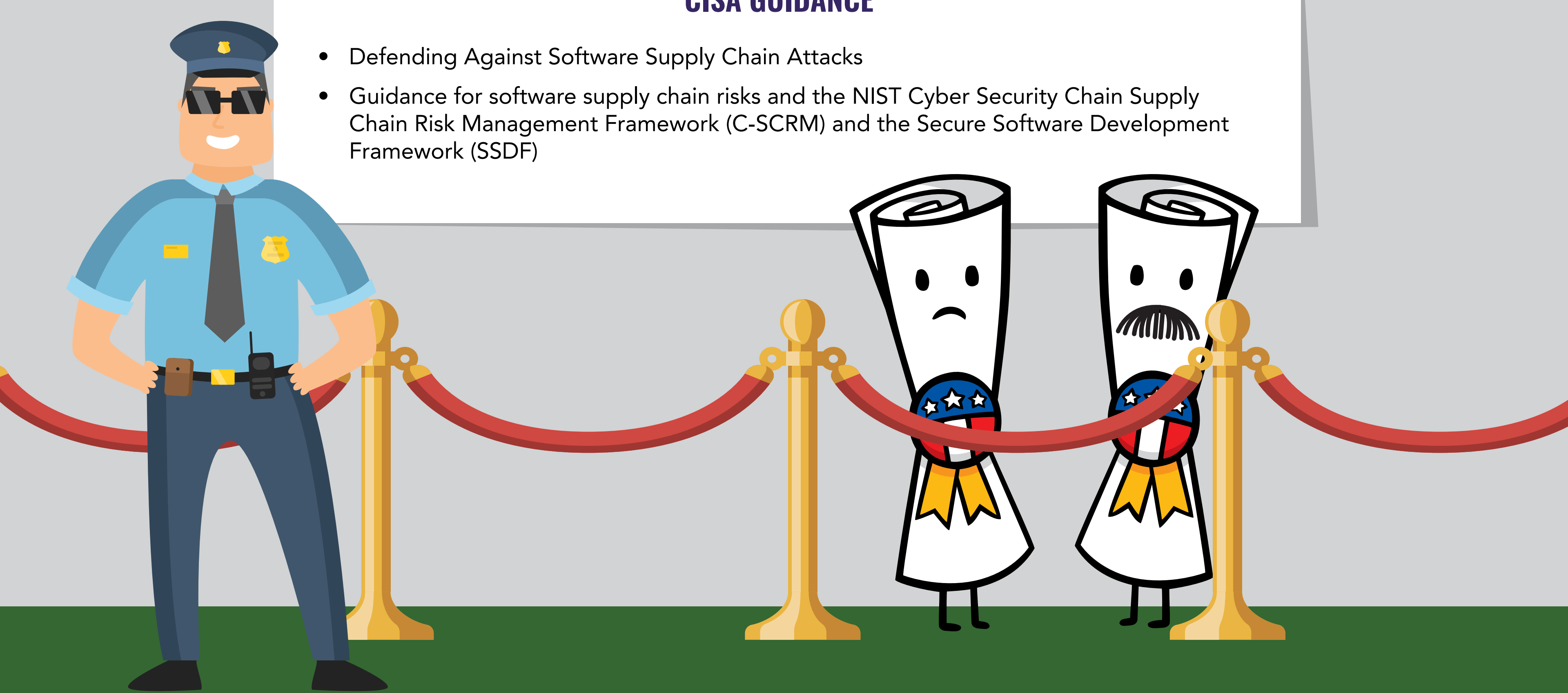
### UN CYBERSECURITY RULES, NORMS AND PRINCIPLES FOR RESPONSIBLE STATE BEHAVIOR

Guidance by the UN to Member States on cybersecurity and threats in the context of international security



### CISA GUIDANCE

- Defending Against Software Supply Chain Attacks
- Guidance for software supply chain risks and the NIST Cyber Security Chain Supply Chain Risk Management Framework (C-SCRM) and the Secure Software Development Framework (SSDF)



## INCREASED INVESTMENT AND ENFORCEMENT ACTIVITIES



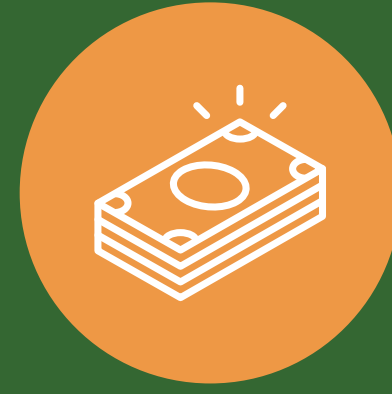
### HIPAA & OCR THIRD-PARTY BUSINESS ASSOCIATE COMPLIANCE ENFORCEMENT

OCR has the authority to take enforcement action against business associates of covered entities for various requirements and prohibitions of the HIPAA Rules



### INCREASING OCR ENFORCEMENT

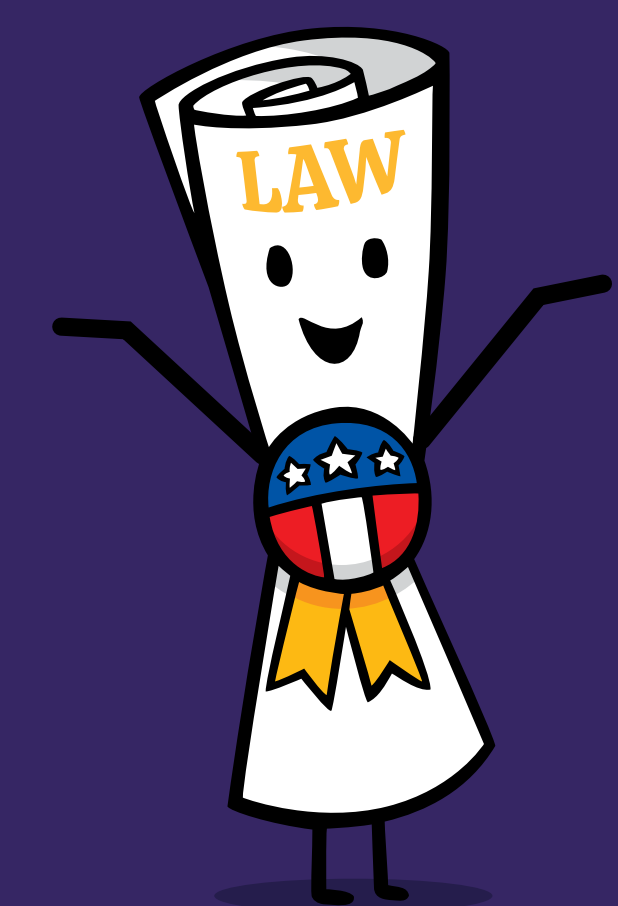
The OCR has indicated its intended ramping of focus on cybersecurity issues and non-compliance enforcement



### PRESIDENT BIDEN'S PROPOSED 2021 BUDGET

- \$9.8B allocated for cybersecurity
- Increased budget over 2020 includes \$1.2B more for the Civilian department and \$750M for SolarWinds attack response

## CONTACT YOUR LOCAL MEDITOLOGY REPRESENTATIVE



- ✓ Gets results by driving vendors to risk reduction
- ✓ Make informed supply chain risk decisions
- ✓ Drive and track remediation
- ✓ Accelerate assessment turnaround times
- ✓ Scale vendor risk programs
- ✓ Validate controls and gain assurance
- ✓ Less cost, more coverage, & higher quality risk outcomes
- ✓ Tech automation + data + services = risk reduction

Meditology Services is a top-ranked provider of information risk management, cybersecurity, privacy, and regulatory compliance consulting services, exclusively for healthcare organizations. Meditology advises healthcare entities of all shapes and sizes.

To learn more about Meditology Services, visit [meditologyservices.com](https://www.meditologyservices.com) and follow us on [LinkedIn](#).



VISIT **MEDITOLOGYSERVICES.COM**  
AND FOLLOW US ON **LINKEDIN**