#RSAC

RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **DSO-M06**

Is a Secure Software Supply Chain Possible – Let Alone Feasible?

Tony Sager

Senior Vice President & Chief Evangelist
Center for Internet Security
@cisecurity

Steve Lipner

Executive Director
SAFECode
@Lipner

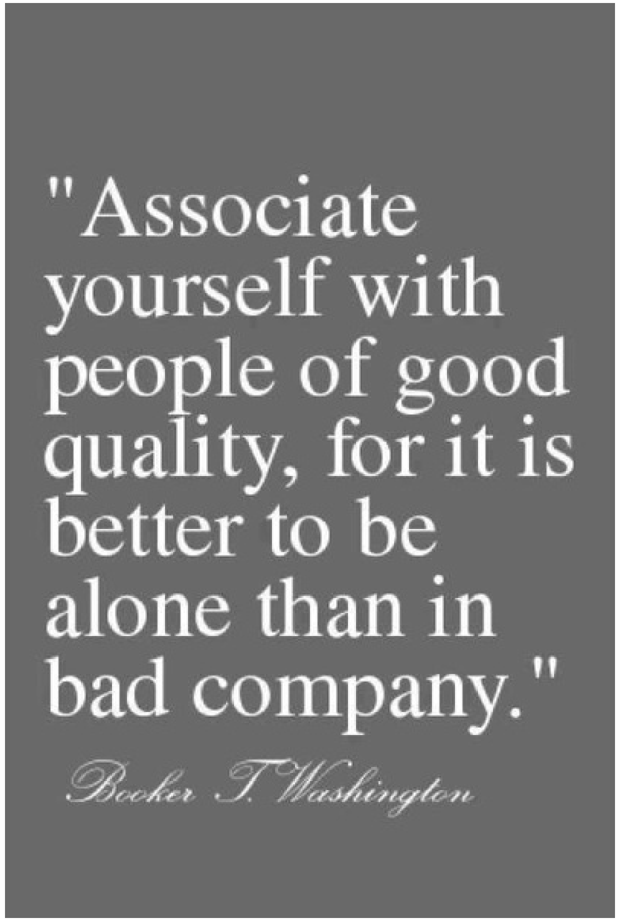
Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Protecting Your Company from the Company It Keeps

- ✓ Business is increasingly interconnected and interdependent via software.
- ✓ The bad guys have figured that out. So have the regulators.
- ✓ The “app cloud” exacerbates that trend, with additional levels of “parties.”
- ✓ Merger and acquisition success depends on cybersecurity levels.
- ✓ Software security/quality is a key factor in business success.



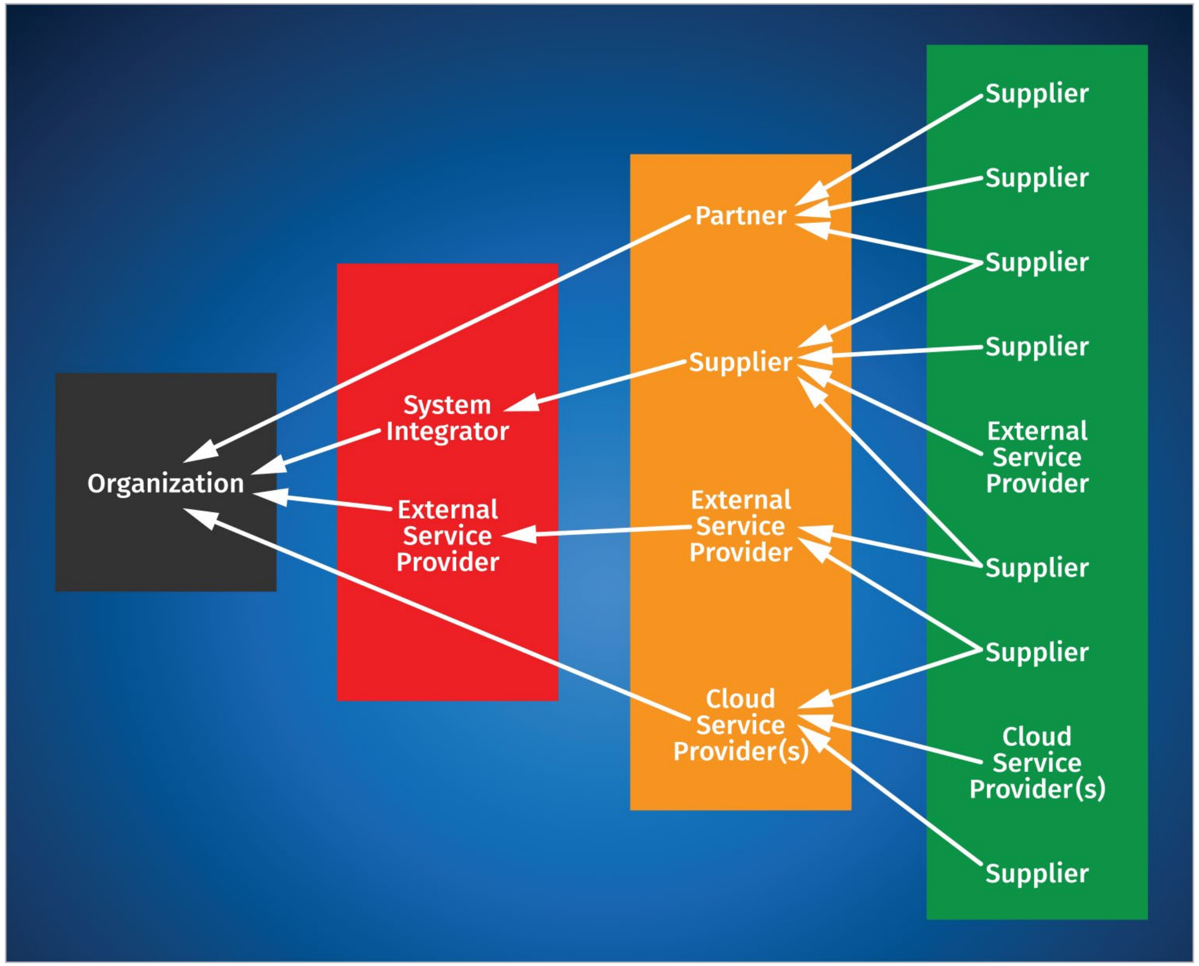
"Associate yourself with people of good quality, for it is better to be alone than in bad company."

Booker T. Washington

CIS

01010
0100000
010001
01000
0100001
SAFECode

It Is Really a Supply Web of Chains

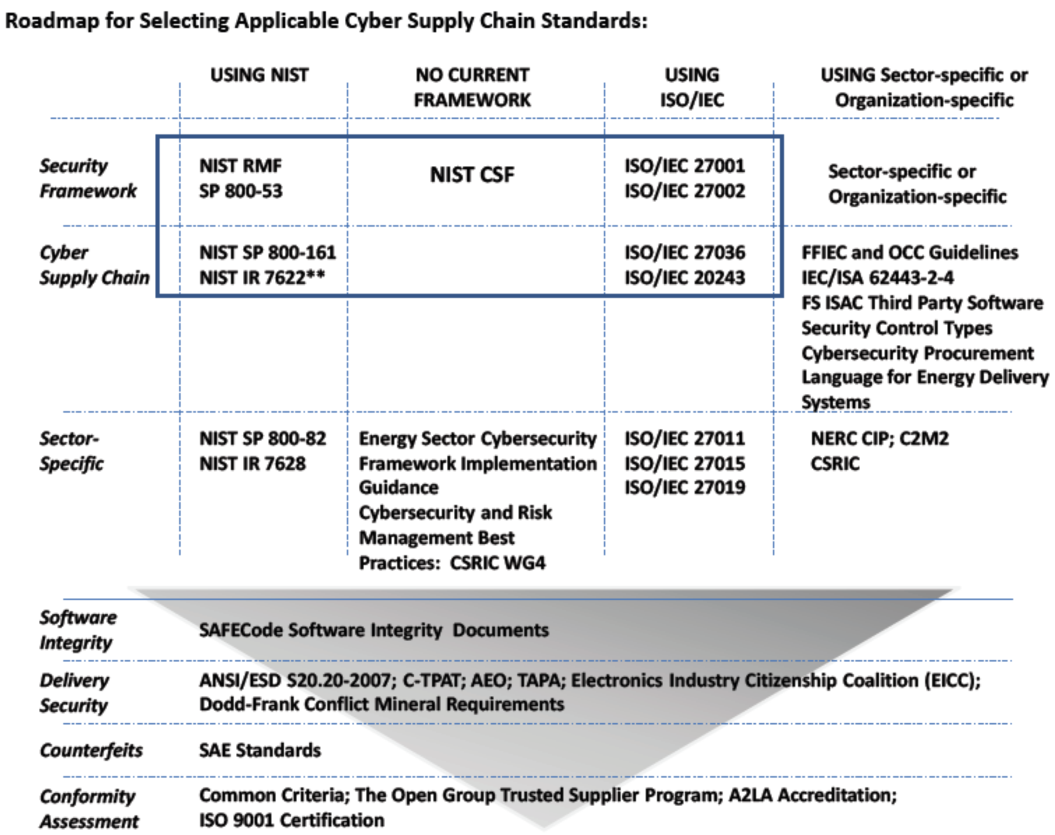

Organization
System Integrator
External Service Provider
Partner
Supplier
External Service Provider
Cloud Service Provider(s)
Supplier
Supplier
Supplier
Supplier
External Service Provider
Supplier
Supplier
Cloud Service Provider(s)
Supplier

from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

What Can Go Wrong?

- Malicious supplier
- Buggy/vulnerable software
- Unauthorized modification in development or delivery
- …at any level in the supply chain

No Shortage of Standards



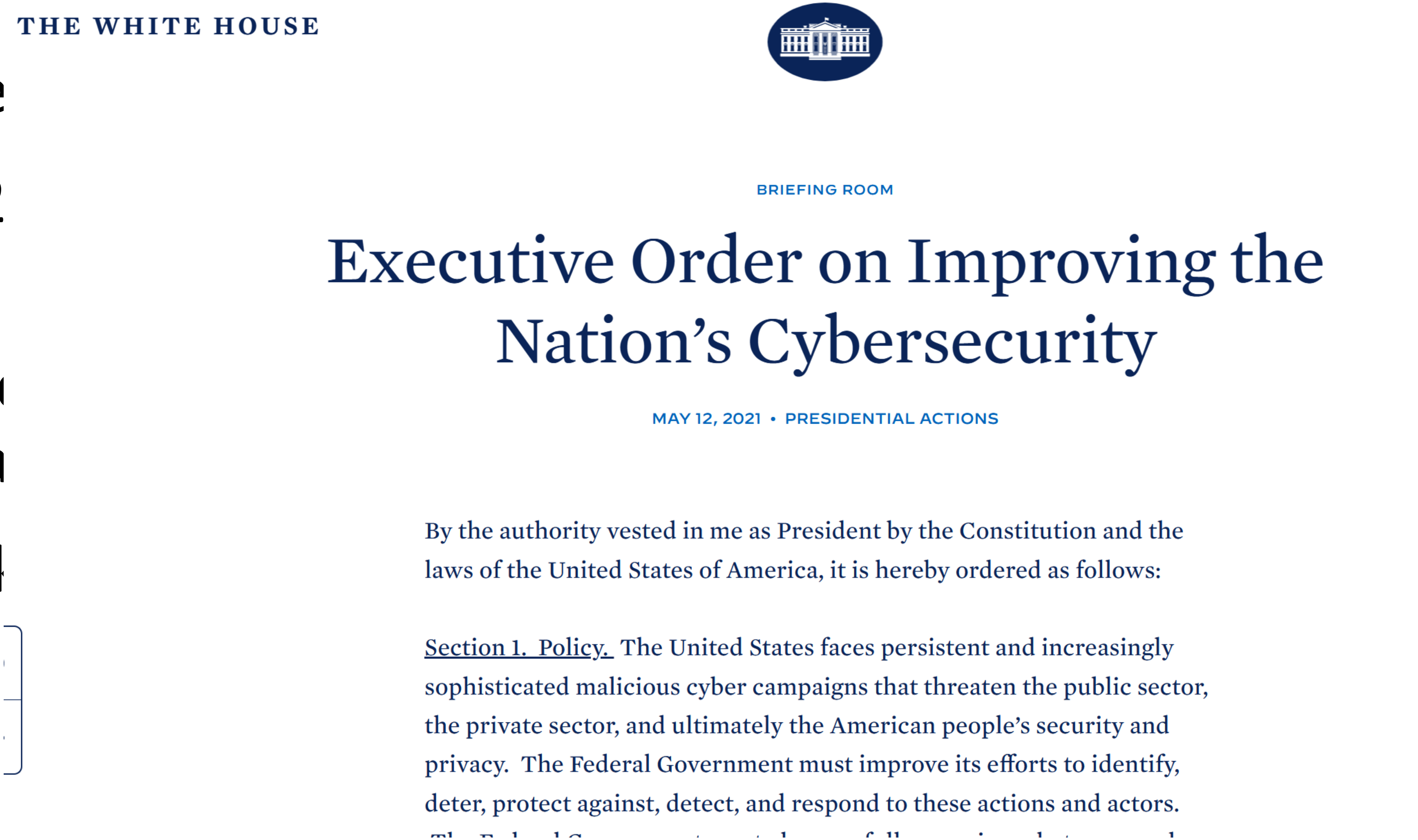
Roadmap for Selecting Applicable Cyber Supply Chain Standards:

	USING NIST	NO CURRENT FRAMEWORK	USING ISO/IEC	USING Sector-specific or Organization-specific
Security Framework	NIST RMF SP 800-53	NIST CSF	ISO/IEC 27001 ISO/IEC 27002	Sector-specific or Organization-specific
Cyber Supply Chain	NIST SP 800-161 NIST IR 7622**		ISO/IEC 27036 ISO/IEC 20243	FFIEC and OCC Guidelines IEC/ISA 62443-2-4 FS ISAC Third Party Software Security Control Types Cybersecurity Procurement Language for Energy Delivery Systems
Sector-Specific	NIST SP 800-82 NIST IR 7628	Energy Sector Cybersecurity Framework Implementation Guidance Cybersecurity and Risk Management Best Practices: CSRIC WG4	ISO/IEC 27011 ISO/IEC 27015 ISO/IEC 27019	NERC CIP; C2M2 CSRIC
Software Integrity	SAFECode Software Integrity Documents			
Delivery Security	ANSI/ESD S20.20-2007; C-TPAT; AEO; TAPA; Electronics Industry Citizenship Coalition (EICC); Dodd-Frank Conflict Mineral Requirements			
Counterfeits	SAE Standards			
Conformity Assessment	Common Criteria; The Open Group Trusted Supplier Program; A2LA Accreditation; ISO 9001 Certification			

Source: NIST 800-161

Changing Landscape (Maybe)

- US Gove … curity
- EO 1402 … nd supply c
- Assuran … , potentia … tions
- If it worl …



THE WHITE HOUSE

BRIEFING ROOM

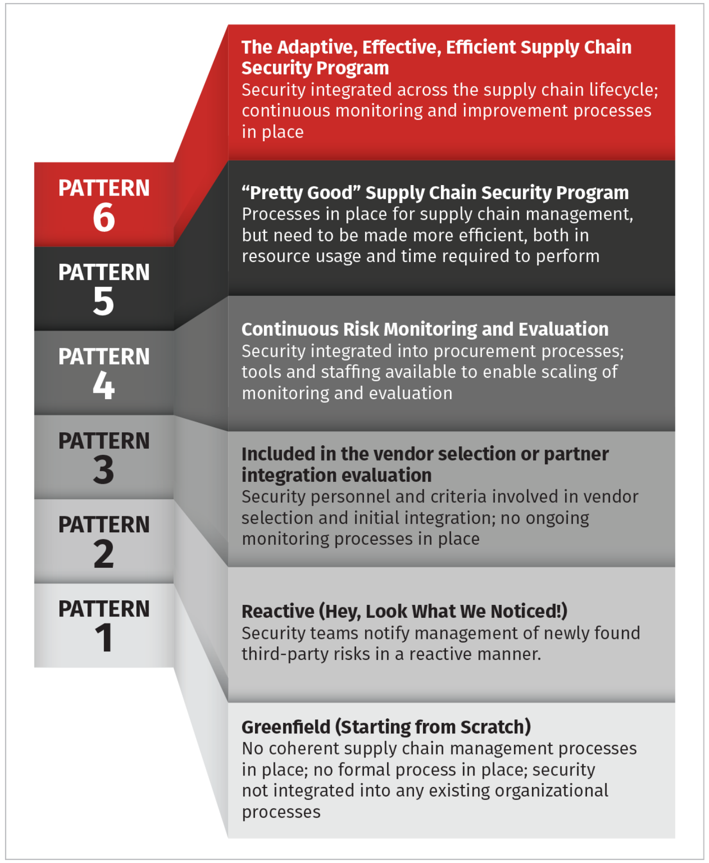
Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors.

CIS 01010 0100000 010001 01000 0100001 SAFECode



The Adaptive, Effective, Efficient Supply Chain Security Program
Security integrated across the supply chain lifecycle; continuous monitoring and improvement processes in place

"Pretty Good" Supply Chain Security Program
Processes in place for supply chain management, but need to be made more efficient, both in resource usage and time required to perform

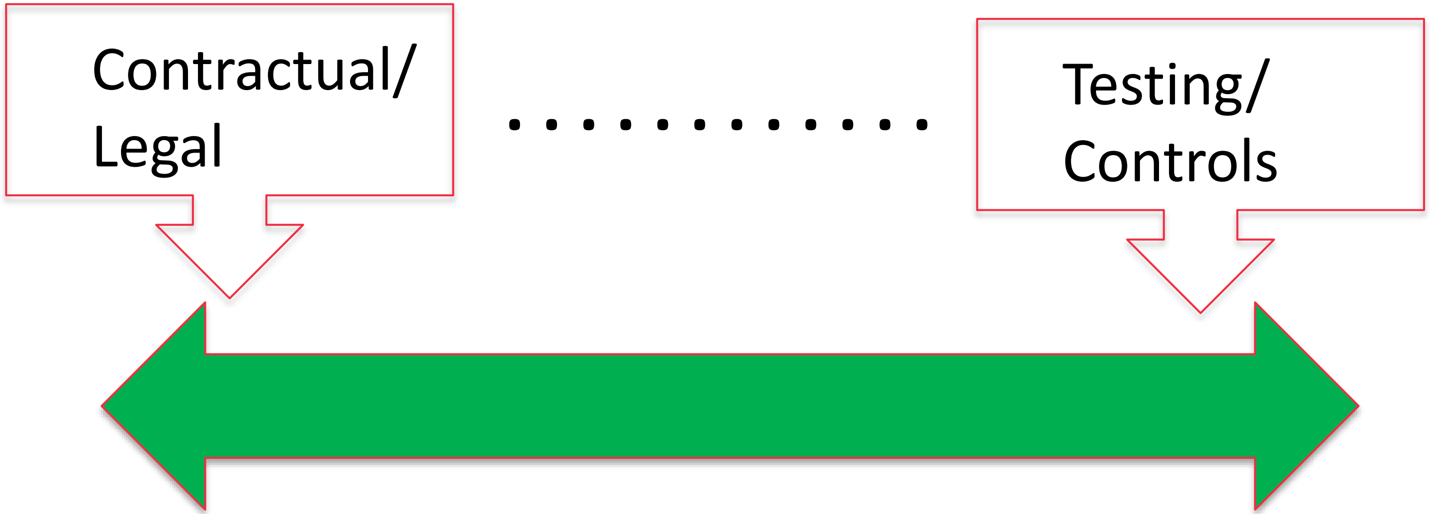
Continuous Risk Monitoring and Evaluation
Security integrated into procurement processes; tools and staffing available to enable scaling of monitoring and evaluation

Included in the vendor selection or partner integration evaluation
Security personnel and criteria involved in vendor selection and initial integration; no ongoing monitoring processes in place

Reactive (Hey, Look What We Noticed!)
Security teams notify management of newly found third-party risks in a reactive manner.

Greenfield (Starting from Scratch)
No coherent supply chain management processes in place; no formal process in place; security not integrated into any existing organizational processes

Starting Point



Contractual/ Legal

Testing/ Controls

Action/Change

How To Tell

- Certifications?
- Supplier documentation
- Testing?
- Continuous improvement?
- What about Open Source?

“Theories of security come from theories of insecurity…”

- Rick Proto, NSA

Today's Discussion

- If you are just getting started, what is most important first step?
- Realistic ways to push security requirements onto software suppliers.
- What about testing/certification of software?

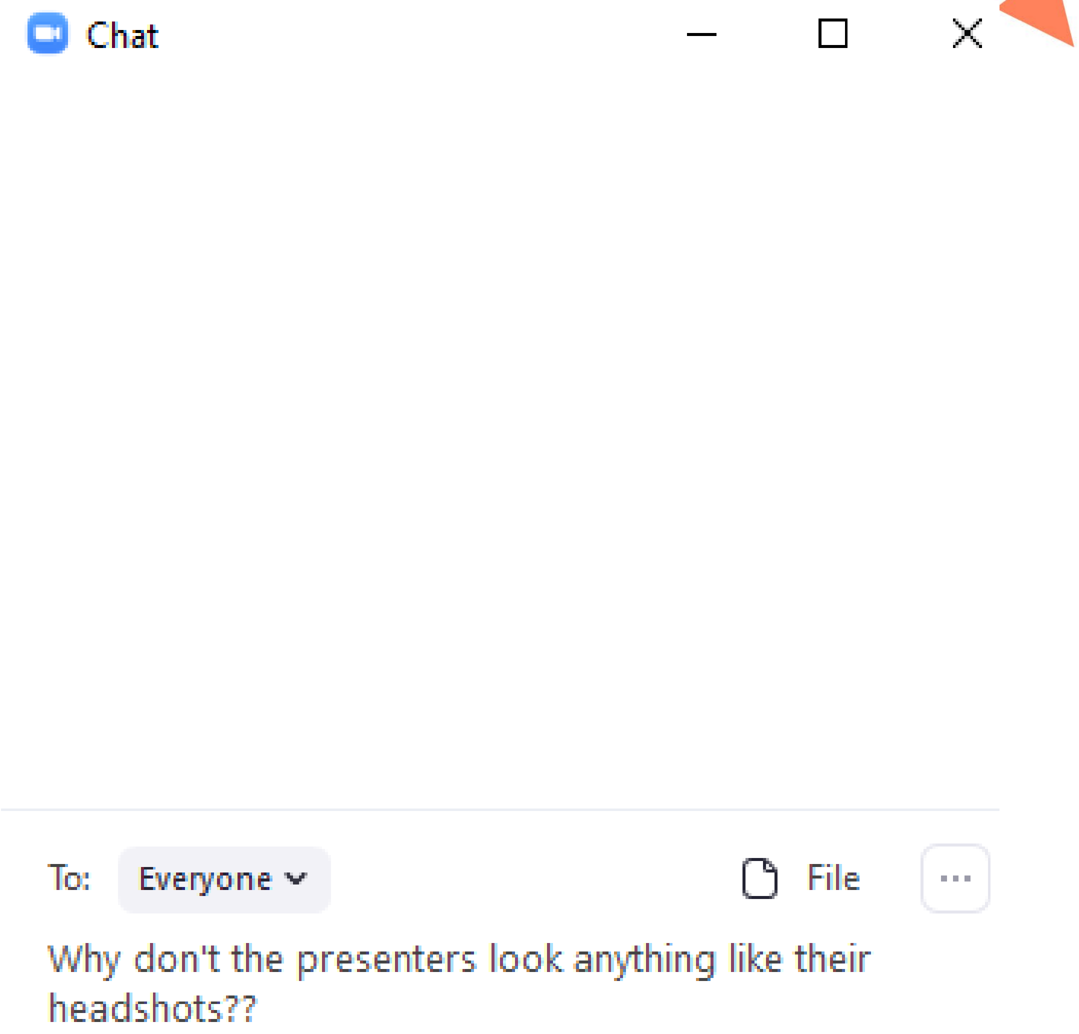
Action: When You Get Back to Work

- Next week you should:
  - Do a realistic assessment of the maturity of your supply chain software security program and reachable and stretch goals.
- In the first three months following this presentation you should:
  - Identify accelerated monitoring/response for showstoppers
  - Understand your in-house software organization's posture for secure development and third-party code
  - Make friends in procurement and legal departments
  - Gain approval for a supply chain steering committee

Action: When You Get Back to Work

- Within six months you should:
  - Get an internal commitment to secure software.
  - Require something in all contracts.
  - Do your first spot-checks of software from suppliers
  - Do a table top exercise with your Board of Directors.
- For more suggestions, see CIS Control #16 and SAFECode companion paper

We love questions – ask us anything!



Why don't the presenters look anything like their headshots??

CIS

01010
0100000
010001
01000
0100001
SAFECode