The 60-Minute Security Audit: A Leader's Framework for Managing Third-Party Risk

IAM Tech Talk Part 3

April 15, 2026

Zach Rattner, Yembo

To Ensure Compliance with Antitrust Laws:

Discussion, comments, and presentations during IAM functions must not:

1. refer to any past, present, or future rates, prices or anything related thereto
2. include any reference to marketing strategies that would reduce competition
3. include any discussion of boycotts of any person, product, or firm
4. inhibit any member's employees from discussing employment with other member companies.

ZACH RATTNER

THE 60-MINUTE SECURITY AUDIT™

Bulletproof your moving operations against cyber threats

April 15, 2026

Disclaimer & Notice

Informational Purposes Only

The content of this presentation is for general educational and informational purposes only. It does not constitute formal legal, cybersecurity, or compliance advice.

Not a C3PAO

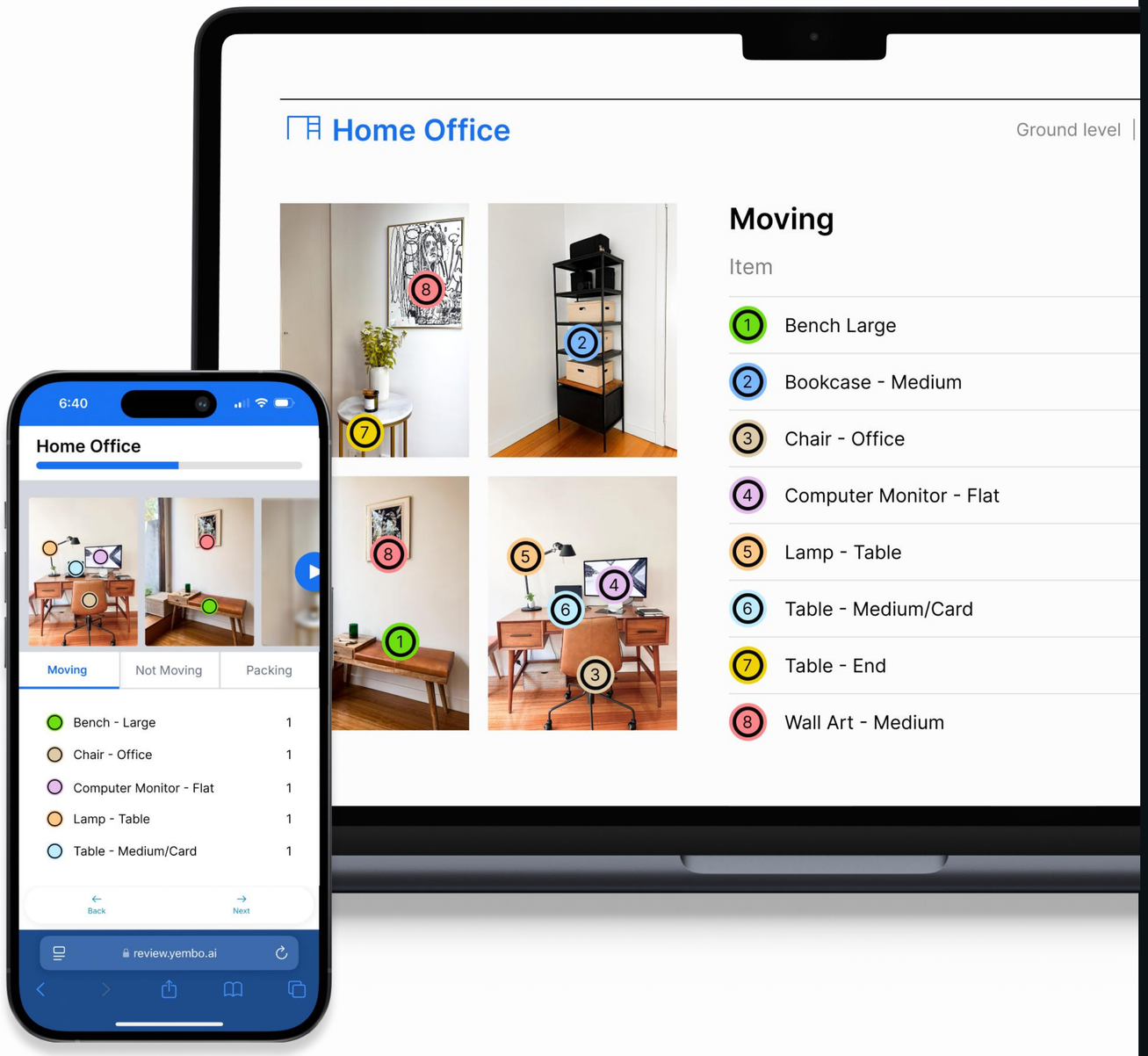
I am not a Certified Third-Party Assessor Organization (C3PAO), nor do I represent the DoD, the Cyber AB, or any official accreditation body. All discussions regarding Cybersecurity Maturity Model Certification (CMMC), SOC 2, ISO 27001, or other compliance frameworks represent my own views and industry observations. Please consult a registered C3PAO or qualified compliance professional for official assessments specific to your organization.

AI Founder, Author, International Keynote Speaker

- Chief Technology Officer & Co-Founder of Yembo
- Author of Grow Up Fast: Lessons from an AI Startup
- International keynote speaker represented by Silicon Valley Speakers, represents Siri and Shazam founders
- BS Computer Engineering, Virginia Tech
- Ex-Qualcomm, 5 years, joined when LTE launched
- 30 granted US patents with several more pending

BACKGROUND

Why moving companies are now prime targets



Movers collect valuable data

A BUNCH OF RULES

A HEALTHY CULTURE

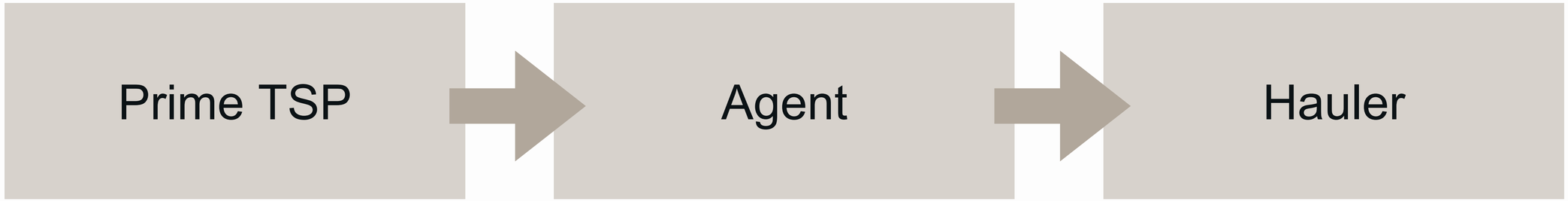
ADVISORY

#26-0025A

Source: https://www.ustranscom.mil

The CMMC mandate flows down.

TSPs will be required to ensure their subcontractor network (agents, haulers, packers, and underlying service providers) complies with the required CMMC level.



If a third-party vendor or a local hauling agent gets breached and exposes government data, the TSP is on the hook. *You can no longer afford to ignore your partners' security hygiene*.

72:00:00

Source: Federal Register

THE AUDIT

Thinking like an attacker

110

Practices required by CMMC 2.0 Level 2

Source: defense.gov

THE FIXES

Low effort, high impact defenses

DRAFT SSP

The foundational blueprint of your compliance strategy. The SSP defines your system boundaries and documents exactly how every security control is implemented to protect Controlled Unclassified Information. It is the very first document an auditor will request.

NIST provides a template.

01

REQUIRE MFA

Your strongest technical defense against unauthorized access. Enforcing MFA for all network and local access across your organization drastically reduces the risk of data breaches caused by compromised passwords.

02

TRAIN SECURITY

Transform your employees from potential vulnerabilities into your primary line of defense. Consistent training ensures your team understands the risks associated with their actions, mitigating the human error that leads to most cyber incidents.

03

Good (and Free) Resources*

*I don’t have any affiliation with these companies

01 NSA Cybersecurity Services

02 Qualys SSL Test

03 Security Headers by Snyk

04 Valimail Domain Checker

DRILL BABY

DRILL!

SECURITY AWARENESS

Use routine simulated phishing tests to turn employees into human firewalls. Regular drills dramatically decrease the likelihood of a real credential harvest or ransomware attack.

01

INCIDENT RESPONSE

Conduct recurring tabletop exercises to ensure everyone knows their exact role during a critical event (like a breach or system outage), speeding up response and recovery times.

02

DATA RECOVERY

A backup plan isn't real until it's tested. Regularly 'drilling' restoration procedures guarantees that systems can actually recover from failure, minimizing costly downtime.

03

THE ROAD AHEAD

Your next 30 days

Recommended next steps

01 Download the audit

https://zachrattner.com/resources/60-minute-security-audit

02 Share with 3 top vendors

03 Start requiring credentials

A BUNCH OF RULES

A HEALTHY CULTURE

ZACH RATTNER

zach@zachrattner.com

@zachrattner