COUNTERINTELLIGENCE WEBINAR SERIES

SUPPLY CHAIN RISKS AND COUNTERINTELLIGENCE

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

TODAY'S SESSION

CDSE Host:

- **Tom Gentle**, Counterintelligence Curriculum Manager

Guest Speakers:

- **Jeanette McMillian**, Assistant Director for Supply Chain and Cyber Directorate, National CI and Security Center – NCSC

- **Chad Bahan**, Asst Director, Insider Threat SCRM, Cybersecurity Services Staff, Office of Chief Information Officer, U.S. Department of Justice

- **Kristoffer J. Buquet**, Chief, Research Development & Acquisition Protection, OUSD (I&S), DDI (CL&S)

ADMINISTRATIVE REMINDERS

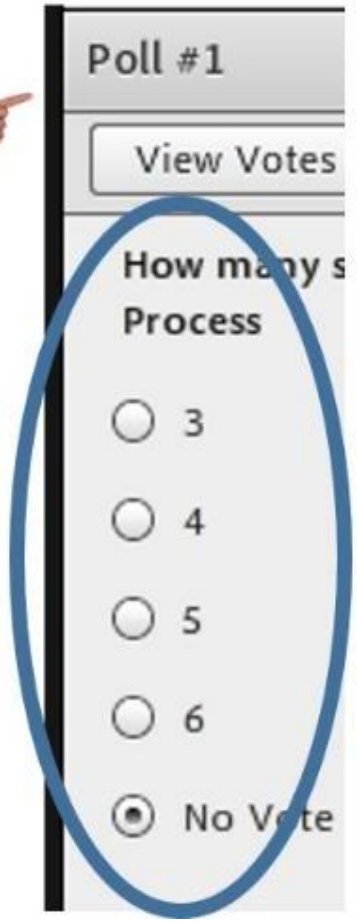
WEBINAR RECORDING -Today's webinar will be recorded in its entirety and made available later on the CDSE website.

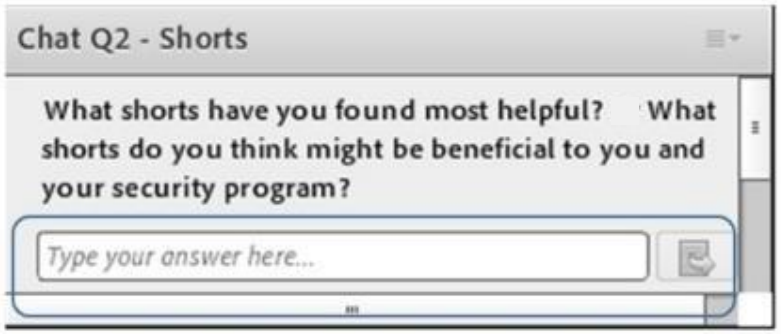
CLASSIFICATION – The webinar event is UNCLASSIFIED in its entirety. All questions and responses to questions will also be unclassified. NO CUI is permitted.

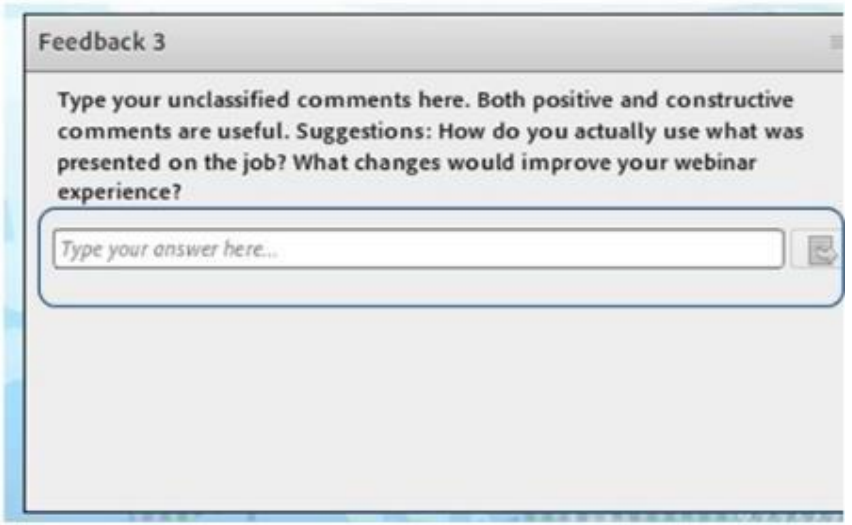
ATTENDEE PARTICIPATION & FEEDBACK

ATTENDEE PARTICIPATION & FEEDBACK

Polls, Chats, and Feedback







POST EVENT FEEDBACK

At the end of our event, please take a few minutes to share your opinions.

Your feedback helps us improve the quality of our offerings.

Responding will only take a few minutes.

Responding is optional.

Jeanette McMillian

Assistant Director
Supply Chain and Cyber Directorate
National Counterintelligence and Security Center

THREAT LANDSCAPE

THREATS

Supply chain threats target organizations from the following vectors:

Adversarial Ownership

Suppliers may be owned, controlled, or influenced by an adversarial nation-state actor. Will this expose your organization's assets?

Cyber

Cyber threat actors may target your suppliers to gain unauthorized access to your IT assets and systems. What is your supplier's cyber posture? Does it match yours?

Geographical

Global suppliers must abide by the laws of the country in which they operate. Are those countries able to access your assets due to your supplier's global footprint?

Insider

Personnel security checks are in place to protect your employees and assets. But what controls are in place for a supplier's employees?

Physical

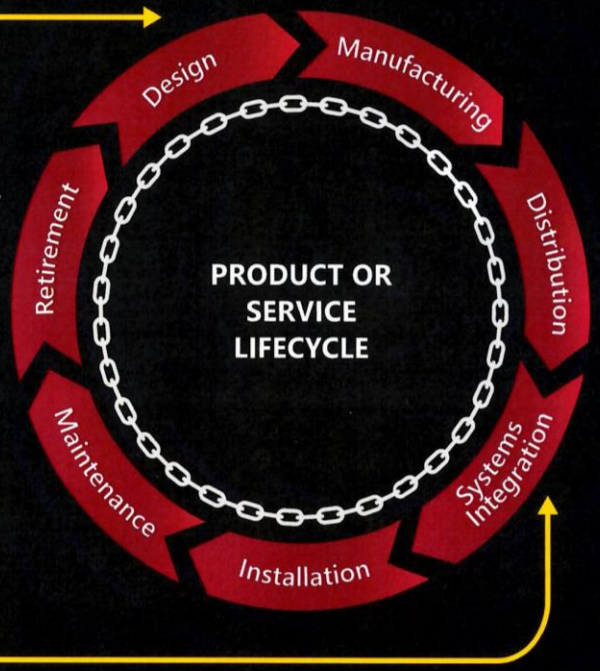
Facility security protocols stop unauthorized access, destruction, or damage to employees and assets. How does your supplier mitigate these same physical vulnerabilities?

Technology

Employees and critical assets operate on IT. Could outdated technology expose your organization or your suppliers' organizations to vulnerabilities that adversaries could exploit?

To address these threats, Supply Chain Risk Management (SCRM) Programs need an A.C.E.: **A**cquisition Security, **C**yber Security, and **E**nterprise Security principles and best practices

METHODS AND POTENTIAL IMPACTS OF SUPPLY CHAIN ATTACKS



ADVERSARIES

- Nation-state actors
- Competitors (especially industry owned or influenced by nation-state actors)
- Malicious insiders
- Criminal organizations
- Hacktivists

If an adversary leverages an opportunity within the supply chain lifecycle, impacts to your organization could include:

- Delayed or degraded production
- Lost intellectual property or competitive business advantage
- Compromised privacy or security
- Disruption of services

COMMON METHODS OF SUPPLY CHAIN ATTACKS

- Cyber compromise
- Theft/interdiction
- Break/fix subversion
- Reroute
- Malicious component insertion
- Repair part compromise
- Trojan insertion/design to fail
- Fraud/counterfeit

SECURING YOUR ECOSYSTEM

CUSTOMER OR BUSINESS PARTNER OPERATIONS THIRD PARTY RISK

If a third-party customer or business partner is compromised, the product or service they are providing may:

- Compromise information systems
- Expose sensitive national security information
- Disrupt or degrade operations
- Result in legal or reputational impacts

#SCRM is the A.C.E.

Acquisition Security | Cyber Security | Enterprise Security

Chad Bahan

Assistant Director
Insider Threat & Supply Chain Risk Management,
Cybersecurity Services Staff
Office of Chief Information Officer
U.S. Department of Justice

Kristoffer Buquet

Chief
Research Development & Acquisition Protection,
Office of the Under Secretary of Defense for Intelligence and Security
Director for Defense Intelligence (CI, LE, and Security)

DDI, CL&S/Information & Acquisition Protection

- E.O. 14107 – America's Supply Chains
- Importance of Supply Chain Due Diligence
- Federal Acquisition Security Council (FASC)
- Information and Communications Technology (ICT)