CUI-CON

SCRM
It Really is a "*Four-Letter*" Word

Carter Schoenberg, CISSP | CCA | QTE

About SoundWay

- ✓ **Cyber AB Authorized C3PAO**

- ✓ **Expert Cybersecurity Professionals**
  - **CMMC Certified Assessor (CCA)**
  - **CMMC Certified Professional (CCP)**
  - **Industry Certifications:**
    - **CISSP • Security+ • PMP • AZURE**
- ✓ **TOP SECRET Facility Clearance**
- ✓ **HUBZone, SDVOSB, WOSB**

- ✓ **FAR & DFARS Compliant or over 12 years**

SOUNDWAY CONSULTING INCORPORATED
("SOUNDWAY")

SoundWay provides information technology, mission support & cybersecurity professional services to the U.S. Department of Defense **(DoD)**, Intelligence Community **(IC)**, federal government civil agencies, and commercial businesses.

SoundWay's commercial business is focused on providing cybersecurity compliance, CMMC certification readiness, & as a C3PAO we are authorized to conduct CMMC certification Assessments.

Since 2018, SoundWay has worked tirelessly to become a leader in cybersecurity; dedicated to demystifying & simplifying Government compliance mandates & making compliance affordable for its fellow contractor community.

MYTHS

- New Concept
- Exclusive to frameworks
- Frameworks dictate outcomes

3.17 – Supply Chain Risk Management

3.17.1 SCRM Plan

3.17.2 Acquisitions Strategies, Tools, and Methods

3.17.3 Supply Chain Requirements and Process


Rule is Published

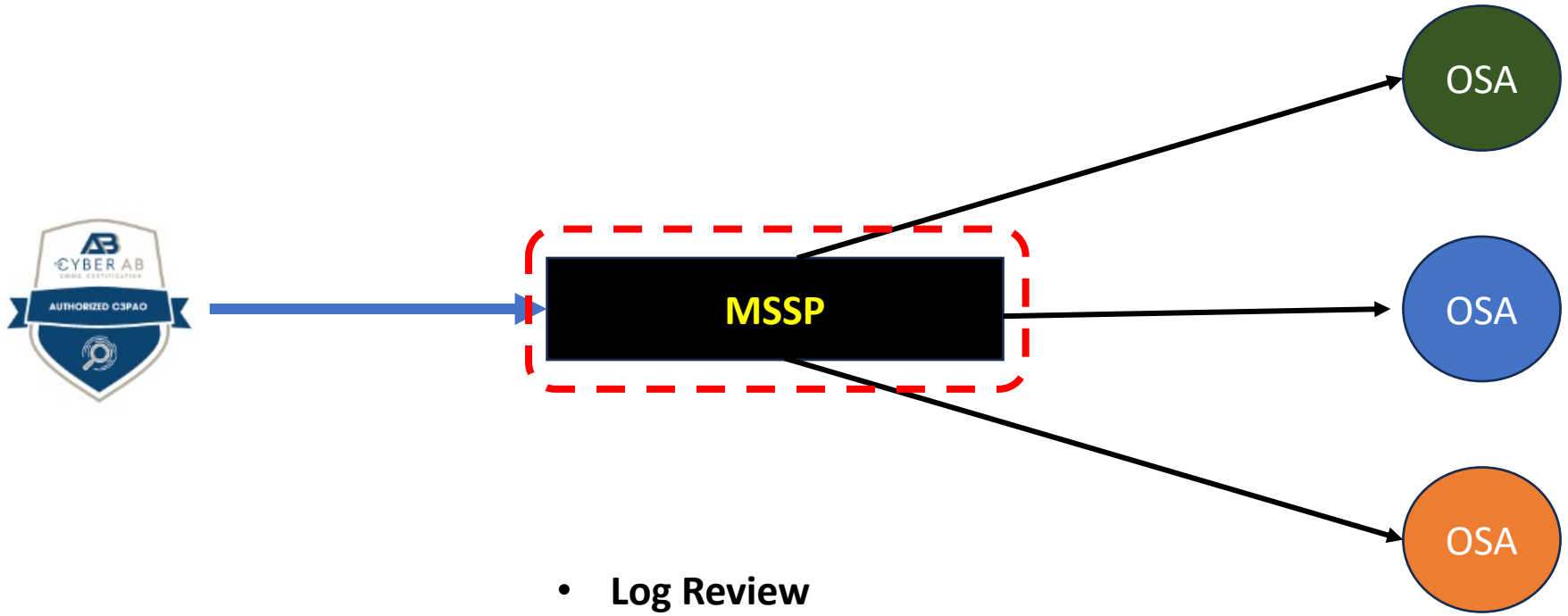
ESPs Hot Topic

(2) If the OSA utilizes an External Service Provider (ESP), other than a Cloud Service Provider (CSP), the ESP must have a CMMC Level 2 Final Certification Assessment. If the ESP is internal to the OSA, the security requirements implemented by the ESP should be listed in the OSA's SSP to show connection to its in-scope environment. In the CMMC Program, CUI or Security Protection Data (e.g., log data, configuration data), must be processed, stored, or transmitted on the ESP assets to be considered an ESP. If using a CSP for Level 2 Self-Assessment, see § 170.16(c)(2). If using a CSP for Level 2 Certification Assessment, see § 170.17(c)(5).

ESPs - Continued

The ESP is now Level 2 Certified, all is good!

Process vs. Reality



- Log Review
- Firewall IDS/IPS Monitoring
- Endpoint Protection
- Vulnerability Scanning

ESPs and L2 Certifications

What can a CMMC L2 IV&V tell you about the services and capabilities an MSP/MSSP provides their clients?

A) The analysis performed by the C3PAO will evaluate all security controls and related objectives subject to NIST SP:800-171r2 that they perform on behalf of their clients.

B) Nothing

C) Banana

Have a Meaningful Dialog

OSA: *"Do you have a CMMC L2 Certification?"*

MSSP: *"We have a CMMC L2 Certification!"*

What should you be asking?

Have a Meaningful Dialog - Continued

OSA: *"Which security controls are you taking over?"*

OSA: *"Which security control objectives are you taking over?"*

OSA: *"Do you have preformed SSP supplementals for me to use?"*

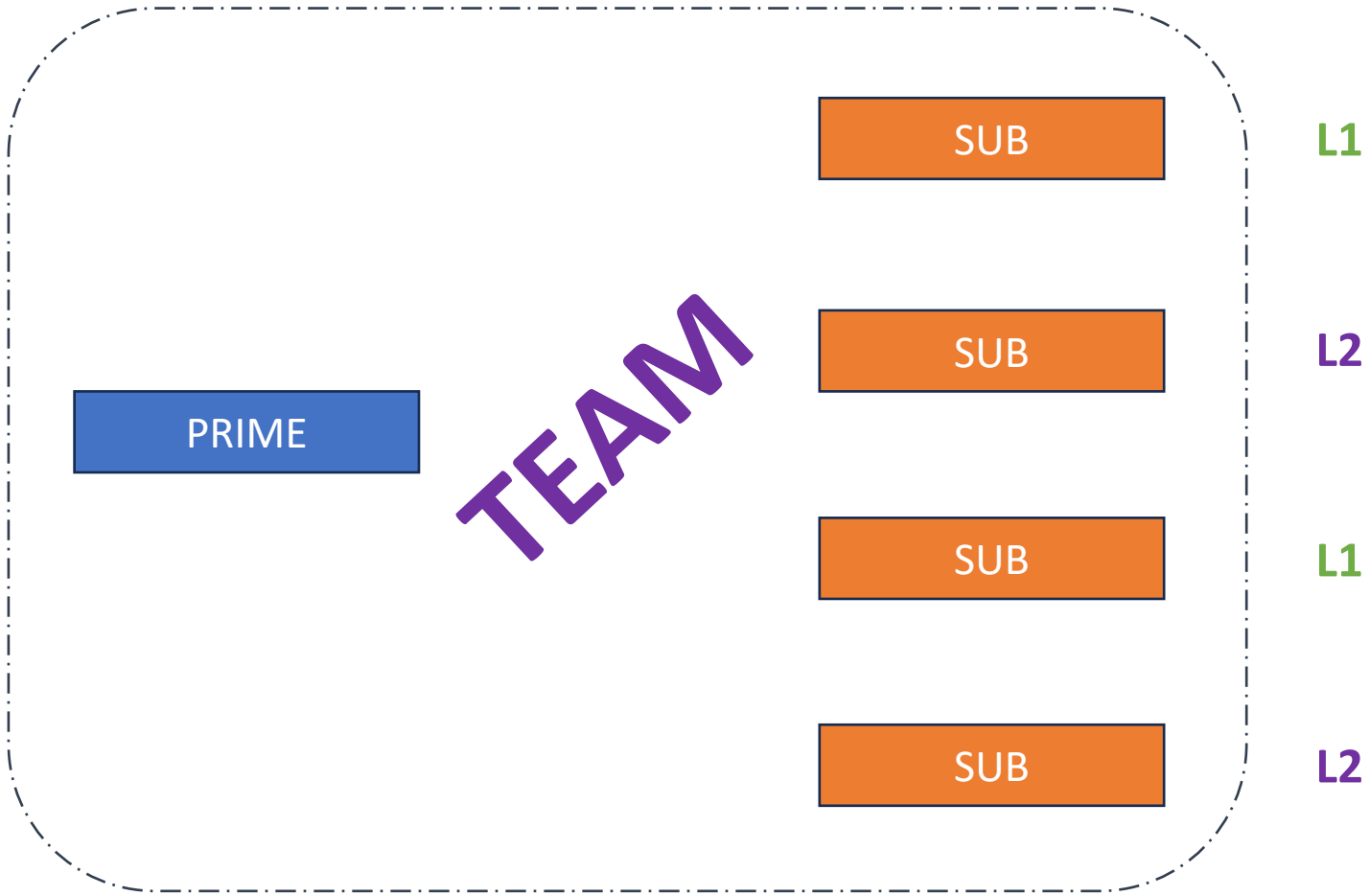
OSA: *"How do you demonstrate SLA conformance?"*

DO NOT

ASSUME

SCRM – Going After DoD Work

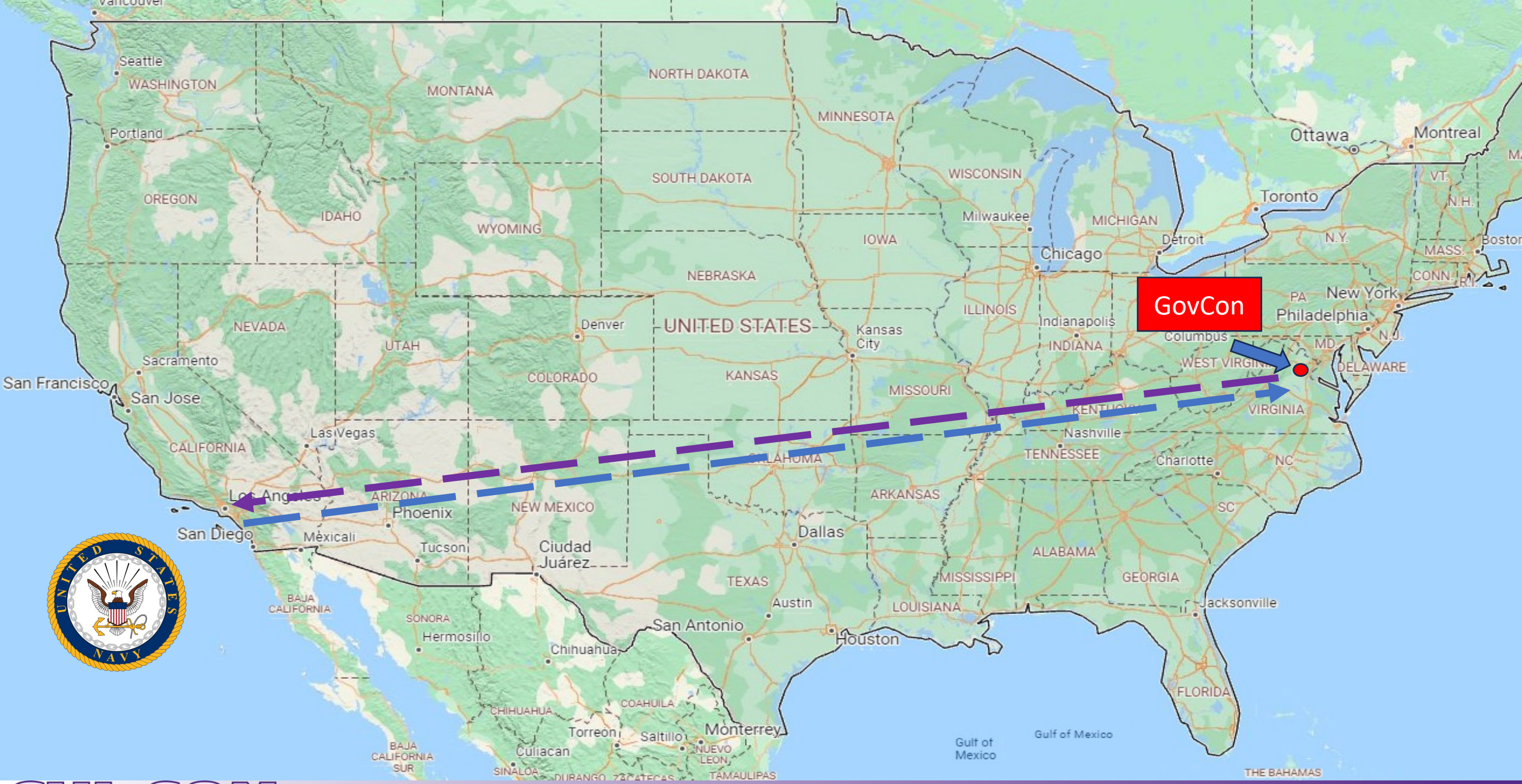
SCRM – Going After DoD Work (Continued)



TEAMING AGREEMENT

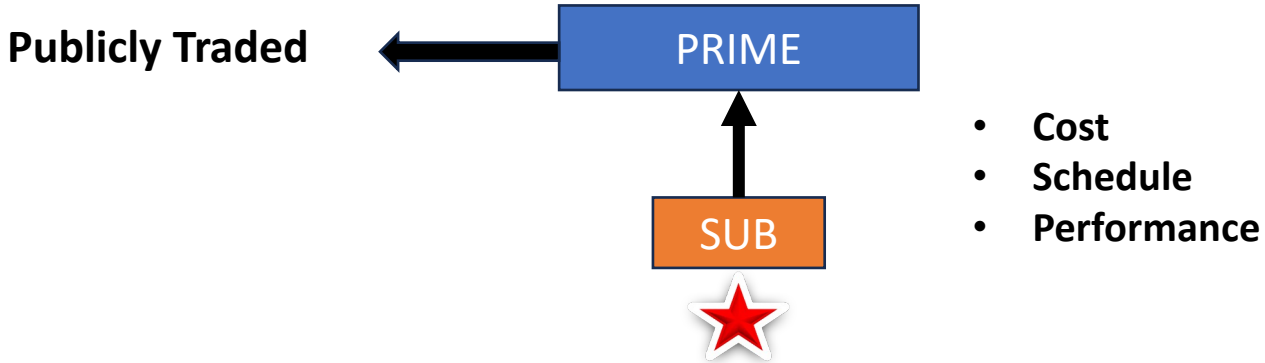
- Proposal Work Assignments
- Work Share
- Pricing
- Commitments
- L2 Certs
- Self Assessment Attestations

WON CONTRACT


GovCon
Seattle
WASHINGTON
Portland
OREGON
IDAHO
MONTANA
NORTH DAKOTA
SOUTH DAKOTA
WYOMING
NEBRASKA
MINNESOTA
IOWA
WISCONSIN
Milwaukee
MICHIGAN
Chicago
Detroit
Ottawa
Montreal
Toronto
VT.
N.H.
N.Y.
MASS.
CONN.
R.I.
Boston
PA
New York
Philadelphia
N.J.
MD.
DELAWARE
VIRGINIA
WEST VIRGINIA
Columbus
Indianapolis
INDIANA
ILLINOIS
Kansas City
Denver
UNITED STATES
NEVADA
UTAH
COLORADO
KANSAS
MISSOURI
Sacramento
San Francisco
San Jose
Las Vegas
CALIFORNIA
Nashville
TENNESSEE
Charlotte
NC
SC
ARKANSAS
ALABAMA
MISSISSIPPI
GEORGIA
Jacksonville
FLORIDA
Dallas
TEXAS
Austin
San Antonio
Houston
LOUISIANA
Los Angeles
ARIZONA
Phoenix
NEW MEXICO
San Diego
Mexicali
Tucson
Ciudad Juárez
BAJA CALIFORNIA
SONORA
Hermosillo
Chihuahua
CHIHUAHUA
COAHUILA
Torreon
Saltillo
Monterrey
NUEVO LEON
TAMAULIPAS
Culiacan
SINALOA
BAJA CALIFORNIA SUR
Gulf of Mexico
Gulf of Mexico
THE BAHAMAS

CUI-CON

It's great – Until it "Isn't"



- **Cost**
- **Schedule**
- **Performance**

BASE | OY 1 | OY 2 | OY 3 | OY 4

It's great – Until it "Isn't" – (Continued)

25,000 Personnel Records "believed" to have been exfiltrated or lost control over

What does the impacted sub and prime have to do?

- **Notify DoD within 72 Hours**
- **Notify CISA within 72 Hours**
- **Notify California Attorney General?**
- **Notify Virginia Attorney General?**
- **Notify Insurance**
- **Notify SEC**

- **Cost**
- **Schedule**
- **Performance**

Questions

C.Schoenberg@soundwayconsulting.us