Cybersecurity Untangled

Strategies for Cybersecurity Compliance

CMMC Day | August 31, 2021

Eric Crusius | Partner, Holland & Knight LLP

Holland & Knight

Introductions: Eric Crusius

Partner

Tysons, VA

703-720-8042

516-314-1307

Eric.Crusius@hklaw.com

Eric Crusius is a partner at Holland & Knight and a government contracts and litigation attorney who focuses his practice on a wide range of government contract matters, including bid protests, claims and disputes, compliance issues (including cybersecurity, supply chain, and labor) and sub-prime issues and manages high-stakes complex commercial litigations.

Eric has appeared as a guest on Fox News, Government Matters TV, NPR, and Federal News Radio and has been quoted in numerous publications including Newsweek, USA Today, the Washington Post, Washington Lawyer, the Financial Times, and the Washington Business Journal.

Twitter: @EricCrusius

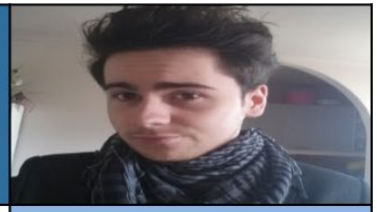
Agenda

Agenda

1. Threats
2. Letters
3. The Tangle
4. The Untangle (Strategies)

Threats

Threats

	**Malware**	**Phishing**	
Denial of Service Attacks		War Driving	**Insiders**
	**Spear Phishing**	Spamming	
Whaling	Spoofing		**Zero-Day Exploits**
		**Terrorists**	

Letters

Where is CMMC Now?

The Tangle

"The Tangle"

- DFARS 252.204-7008
- DFARS 252.204-7009
- DFARS 252.204-7012
- DFARS 252.204-7014
- DFARS 252.204-7019
- DFARS 252.204-7020
- DFARS 252.204-7021
- FAR 52.204-21
- DOSAR 652.239-70
- DOSAR 652.239-71
- IRS Publication 4812
- NFS 1852.204-76
- GSAR 552.239-70
- GSAR 552.239-71
- EO 14028
- EO 13800
- EO 13636
- FISMA
- FITARA
- Breach Notification Laws in 50 States
- SEC
- FTC

- NIST SP 800-216
- NIST SP 800-210
- NIST SP 800-207
- NIST SP 800-172A
- NIST SP 800-172
- NIST SP 800-171A
- NIST SP 800-171
- NIST SP 800-161
- NIST SP 800-160
- NIST SP 800-150
- NIST SP 800-145
- NIST SP 800-144
- NIST SP 800-53

The Untangle

The Untangle

#1 - Look to the Contract

- Most government contracting requirements will be found in a contract.
- The contract will have the requirements including:
  - The FAR Clause
  - Agency Clauses
  - Other Bespoke Requirements

The Untangle

#2 – Understand the Layered Requirements

- Cybersecurity requirements come in layers:
  - Federal contract requirements;
  - State requirements; and
  - Industry-specific requirements.

The Untangle

#2 – Understand the Layered Requirements (con't)

- DFARS 252.204-7012. What is covered defense information? It is "unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—

1. Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or
2. Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract."

The Untangle

#2 – Understand the Layered Requirements (con't)

- Supply Chain Requirements: There are supply chain requirements in CMMC. For instance:
  - Level 2 (SI.2.214): Monitor security alerts, correct information system flaws, and notify supply chain partners.
  - Level 3 (C032; RM.3.146): "Develop and implement risk mitigation plans."
  - Level 4 (C033; RM.4.148): "Develop and update as required, a plan for managing supply chain risks associated with the IT supply chain."
  - Level 5 (C032; RM.5.155): "Analyze the effectiveness of security solutions at least annually to address anticipated risk to the system and the organization based on current and accumulated threat intelligence."
  - Levels 2-5 (C031): Identify and evaluate risk.

The Untangle

#3 – Understand CMMC

- Strategize for CMMC compliance:
  - Review current contracts to determine what level of CMMC certification will be needed;
  - Utilize free resources (including from the CMMC AB); and
  - Follow the latest news:
    - CMMC review ongoing
    - Awaiting final DFARS rule
    - CMMC AB continues to ramp up

The Untangle

#3 – Understand CMMC

(a) Scope. The Cybersecurity Maturity Model Certification (CMMC) CMMC is a framework that measures a contractor's cybersecurity maturity to include the implementation of cybersecurity practices and institutionalization of processes (see https://www.acq.osd.mil/cmmc/index.html).

(b) Requirements. The Contractor shall have a current (i.e. not older than 3 years) CMMC certificate at the CMMC level required by this contract and maintain the CMMC certificate at the required level for the duration of the contract.

(c) Subcontracts. The Contractor shall—

(1) Insert the substance of this clause, including this paragraph (c), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items, excluding commercially available off-the-shelf items; and

(2) Prior to awarding to a subcontractor, ensure that the subcontractor has a current (i.e., not older than 3 years) CMMC certificate at the CMMC level that is appropriate for the information that is being flowed down to the subcontractor.

The Untangle

#4 – Understand the Risks

- This is now a high-risk compliance area:
  - Failure to obtain a CMMC certification means failure to obtain a contract;
  - Look at inconsistent certifications with new SPRS requirements;
  - What happens if there is a cybersecurity breach? Companies can be victims three times over.

The Untangle

#5 – Get a Plan

- Determine whether cybersecurity compliance will be accomplished internally or with the help of third-parties and find the right people to execute.
- Remember CMMC and do not forget other non-CMMC requirements.

The Untangle

#6 – Get Familiar with your Supply Chain

- Draft subcontract agreements that require CMMC certifications and DFARS rquirements. This includes -7012 and -7019 and -7020.
- Allow for unilateral changes when the Government passes on a change.
- Require subcontractors comply with cybersecurity investigations.
- Permit termination if subcontractors do not comply with cybersecurity requirements.
- Smallest companies are most at risk.
- Do not forget about independen contractors.

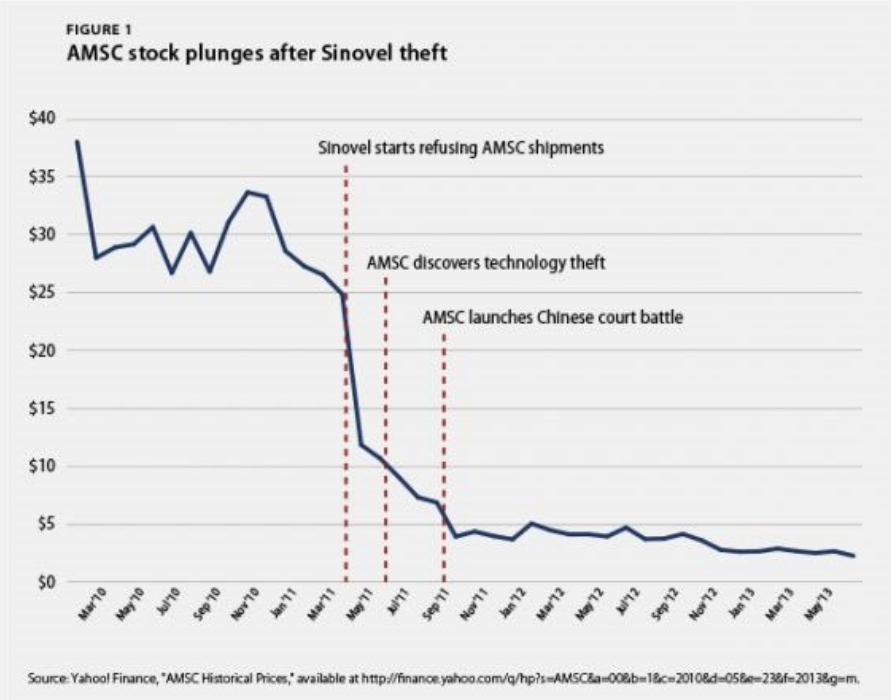
The Untangle

#6 – Get Familiar with your Supply Chain

- The Chinese firm enticed Karabesic to download American Superconductor's encrypted source codes onto a thumb drive and then send them by email to Sinovel executives in China, according to prosecutors.
- As inducements, the emails and Skype messages show, it offered Karabasevic a $1.7 million contract, an apartment in Beijing and access to women -- as well as payments wired into the bank account of a girlfriend who was a Vietnamese flight attendant.
- "All girls need money. I need girls. Sinovel needs me," read one of Karabasevic's messages to a Sinovel executive in China.

The Untangle

#6 – Get Familiar with your Supply Chain



The Untangle

#7 – What to Start Today

1. Review exisiting agreements (prime contracts and subcontracts).
2. Determine if there are areas of non-compliance or risks.
3. Draft a strategic plan to determine cybersecurity compliance path.
4. Subscribe to resources and stay on top of the latest.

Q & A