PUBLIC CONTRACTING INSTITUTE

"Buy America" and Country of Origin Requirements

Session 9: Sanctions and Other Prohibited Sources

David S. Gallacher
Lisa C. Mays
Sheppard Mullin | Supply Chain Team

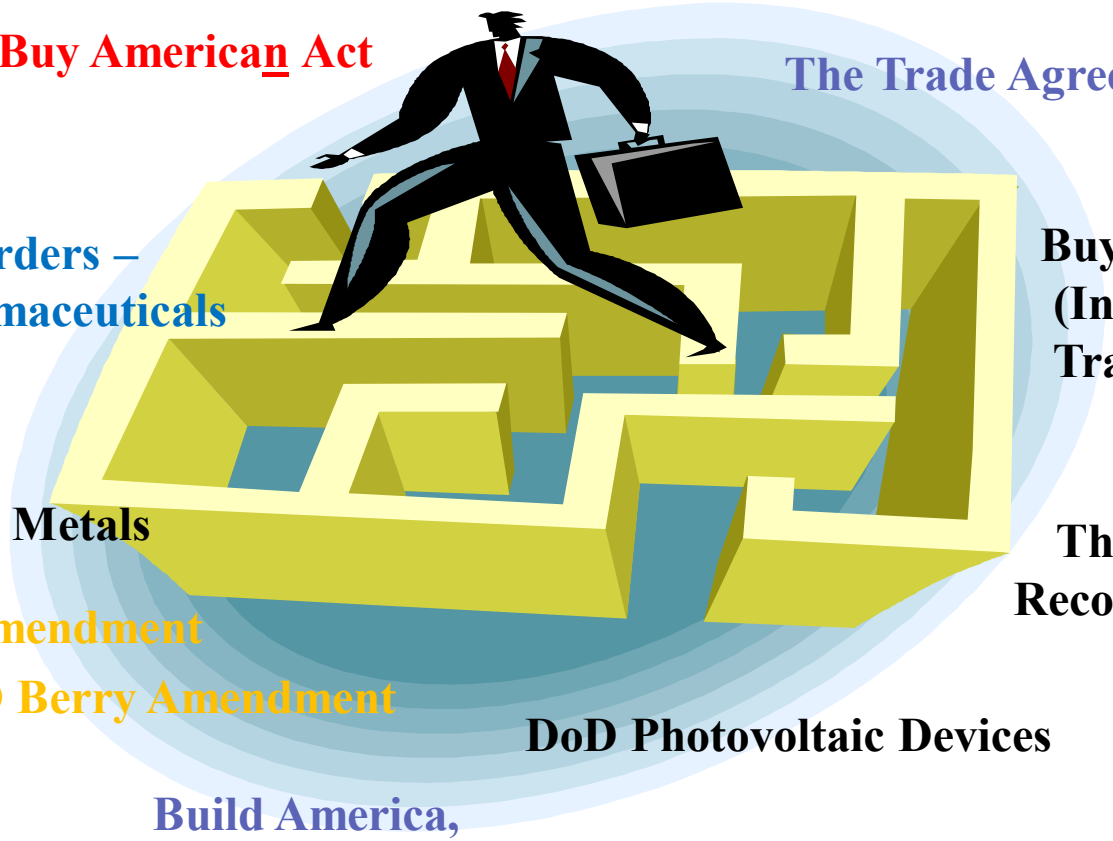
May 10, 2023

Overview of the Series

- January 11: Buy American Act
- January 25: Trade Agreements Act
- February 8: Buy America Requirements under Federally-Funded Transportation Programs
- February 22: Country of Origin Requirements under Federal Grant Programs
- March 8: Customs and "Made in the USA" Labeling
- March 22: The Berry Amendment
- April 12: Specialty Metals Restrictions
- April 26: "Buy America" Round-Up
- May 10: Sanctions and Other Prohibited Sources

INTRODUCTION

The "Country of Origin" Maze



The Buy American Act

The Trade Agreements Act

Executive Orders – Products + Pharmaceuticals

Buy America Act (Infrastructure/ Transportation)

DoD Specialty Metals

The 2009 Recovery Act

DHS Kissell Amendment

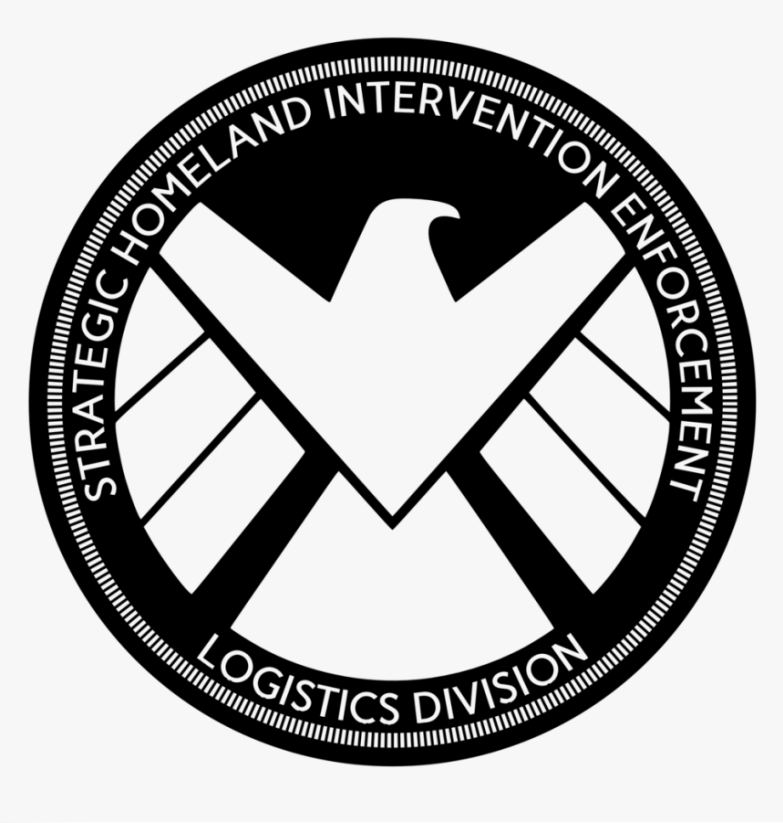
DoD Berry Amendment

DoD Photovoltaic Devices

Build America, Buy America

And Many, Many More…

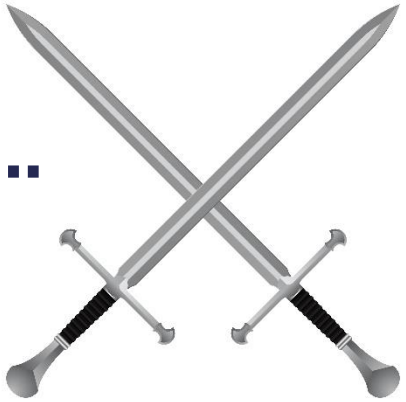
Two Ways To View Country of Origin Restrictions…



Domestic Preferences as a Shield...

- **Buy American Act (BAA)**: **products** sold to the Government under a designated dollar threshold must be manufactured in the United States with a percentage of domestic content
- **Trade Agreements Act (TAA)**: the Government can only purchase **products and services** manufactured or substantially transformed in certain countries

Domestic Preferences as a Sword…



- **Treasury/OFAC Sanctions**
- **Prohibitions against specific companies**
  - Prohibition of Kaspersky software products and services (since 2018)
  - Prohibition against Huawei and ZTE (and others) (since 2019)
- **Prohibitions on entire sectors**
  - Chinese semiconductors (2023 National Defense Authorization Act, Section 5949)
- **Continuing assessment of Supply Chain risk**
  - Federal Acquisition Supply Chain Security Act of 2018
  - FASC Interim Rule (2020) outlines processes and procedures for FASC to evaluate supply chain risk
- **Continued push in Congress to extend this kind of "blacklisting"**

KASPERSKY lab

HUAWEI

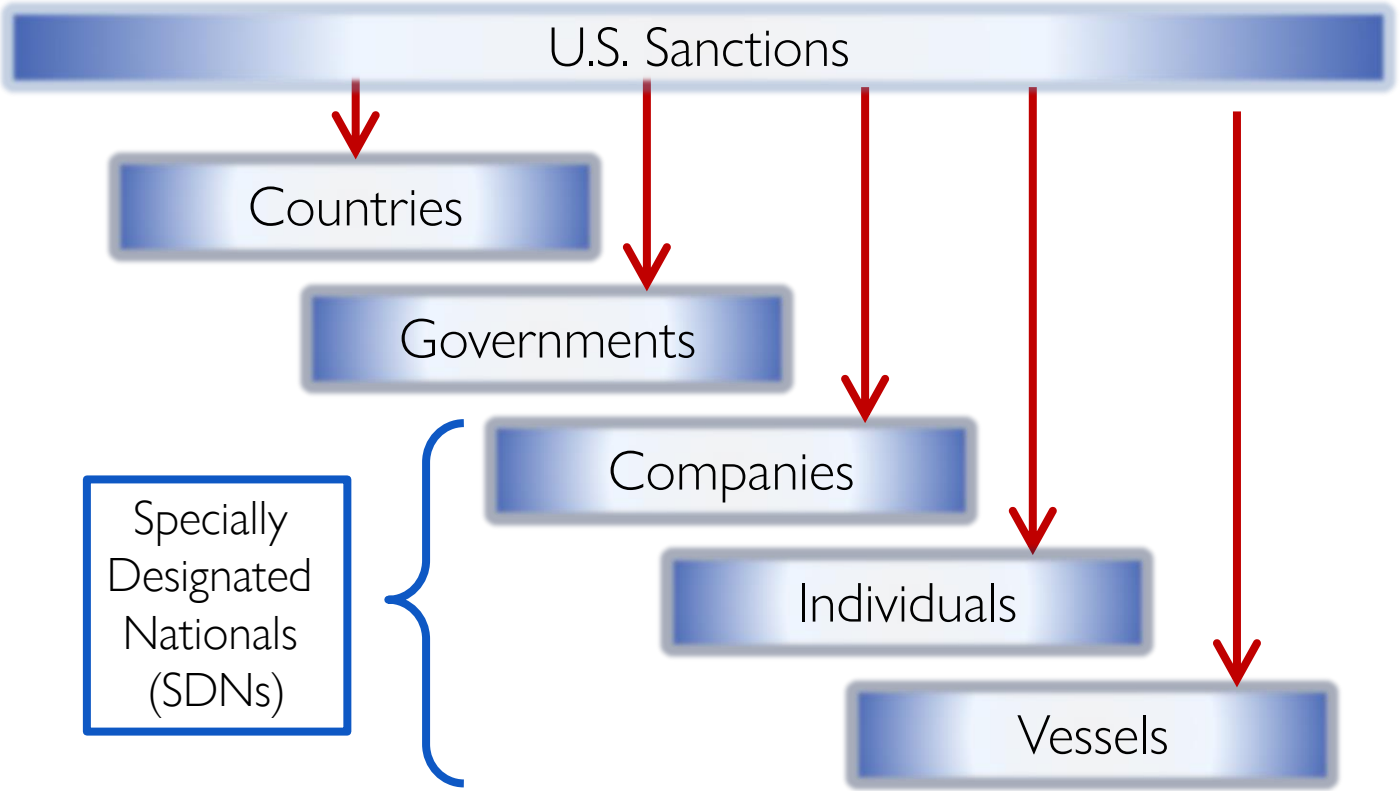
ZTE
中兴通讯股份有限公司
ZTE CORPORATION

Today's Agenda: Sanctions & Prohibited Sources

1. U.S. Sanctions (OFAC + FAR Subpart 25.7)
2. Kaspersky Labs
3. Section 889/Huawei + ZTE
4. Chinese Semiconductors
5. Chinese Forced Labor

1. U.S. SANCTIONS (OFAC + FAR SUBPART 25.7)

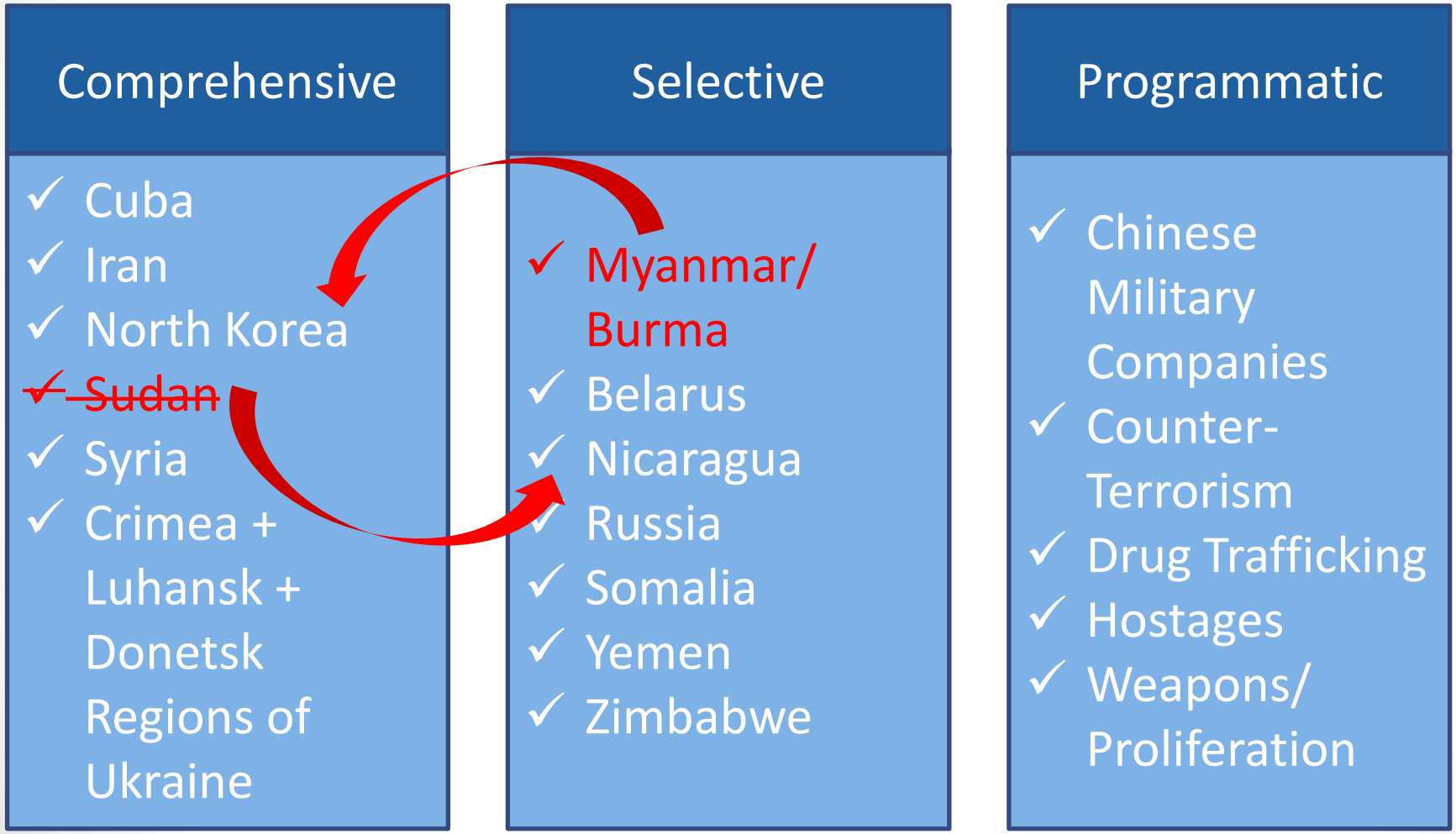
U.S. Sanctions: Overview



U.S. Sanctions: Overview (cont'd)

- Sanctions restrict **transactions** with prohibited parties
- Approximately 30 different U.S. sanctions programs
- Frequent updates
- U.S. Treasury Department, Office of Foreign Assets Control (OFAC)

U.S. Sanctions: Overview (cont'd)



U.S. Sanctions: Various Lists

- Specially Designated Nationals (SDN) List
- Denied Persons List
- Entity List
- Unverified List
- Military End User (MEU) List
- ITAR Debarred List
- Excluded Parties List (SAM.gov)
- Many, many more…

Trade.gov Consolidated Search Engine

FAR-Based Sanctions (FAR Subpart 25.7)

Iran

Cuba

North Korea

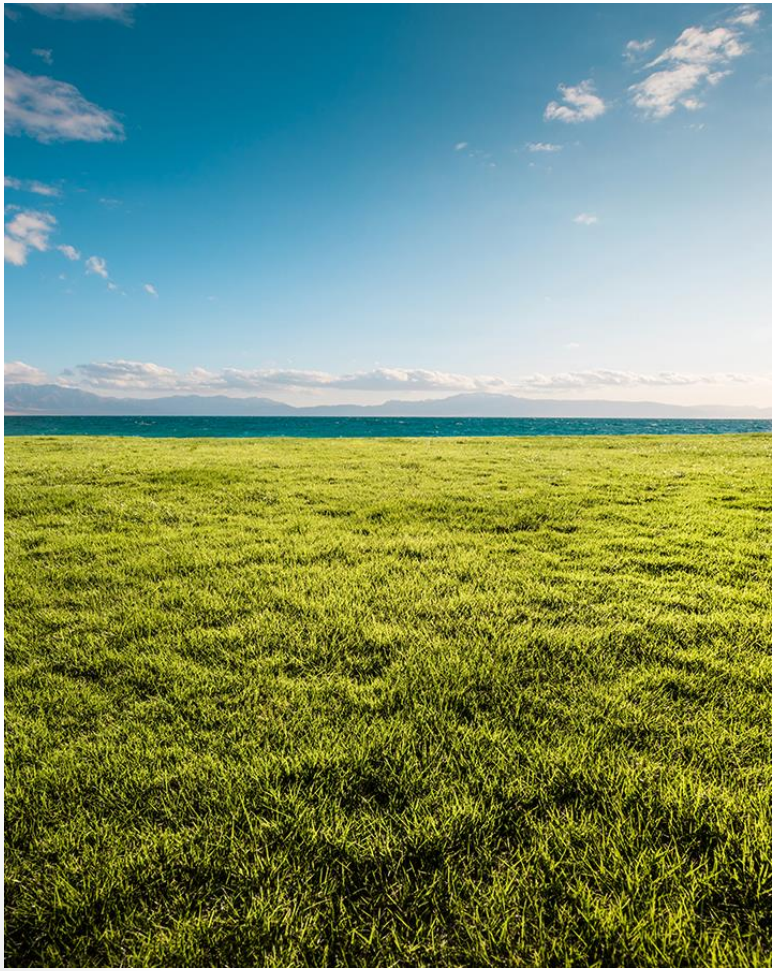
Myanmar/Burma

Sudan

Syria

FAR 52.225-20 and 52.225-25

U.S. Sanctions: Points to Remember



- OFAC jurisdiction is very broad
  - There can be liability for any person, **regardless of nationality**, who causes a violation
- Facilitation/Services Prohibition
  - U.S. person **cannot facilitate or otherwise support** activity that would be prohibited if performed by U.S. person
- SDNs can be located in non-sanctioned countries, *e.g.*, England, Mexico, Qatar

U.S. Sanctions: Best Practices

- Avoid doing business with any of these countries (easiest)
- Flow down prohibition to your suppliers
- Screening (**before** undertaking the new business or sharing technology):
  - Visitors
  - Customers
  - Vendors
  - Other transaction partners
  - Intermediaries
  - Prospective employees

- Risk assessments
  - Identify risk areas (*e.g.*, new customers, geographies)
- Written policies and procedures to manage compliance

2. KASPERSKY LABS

Anti-Kaspersky Labs

- Section 1634 of FY2018 NDAA
- FAR 52.204-23 & FAR Subpart 4.20
- Prohibits hardware, software, and services developed or provided by Kaspersky Lab (Russian cybersecurity company) or related entities

Anti-Kaspersky (cont'd)

- Contractors must report within one business day any covered article discovered during contract performance and provide further details within 10 business days
- Mandatory flowdown to all suppliers
- Screen all customers/vendors for compliance
- Implied certification

3. SECTION 889/HUAWEI + ZTE

Anti-Huawei & ZTE – Section 889

- Section 889 of FY2019 NDAA
- Prevents the sale **or** use of products or services incorporating certain Chinese technology
- Covers products and services that incorporate telecommunications equipment produced by the following companies (plus affiliates):
  - ✓Huawei Technologies Co.
  - ✓ZTE Corp.
  - ✓Hytera Communications Corp.
  - ✓Hangzhou Hikvision Digital Technology Co.
  - ✓Dahua Tech. Co (or any subsidiary or affiliate)

Section 889: FAR Clauses

FAR 52.204-25	FAR 52.204-24	FAR 52.204-26
All ***contracts***	All ***solicitations***	All ***solicitations***
Contractors prohibited from ***providing*** to the USG any covered telecommunications equipment or services ***as a substantial or essential component of any system***, or as a critical technology as part of any system. ***Contractors*** prohibited from ***using*** any telecommunications equipment or services ***as a substantial or essential component of any system***, or as a critical technology as part of any system.	Certification: Offerors to represent whether it ***will/will not provide*** covered telecommunications equipment or services to the USG ***in the performance of the specific contract/subcontract/ solicitation***. Offerors to represent whether does/does not use covered telecommunications equipment or services.	Certification: Offerors must represent whether it ***does/does not provide*** covered telecommunications equipment or services to the USG, ***generally, whether as a prime or subcontractor***. Offerors must represent whether it does/does not use covered telecommunications equipment or services.

Section 889: 2 Prohibitions

Part A

- Prohibits contractors from ***selling*** to the Government equipment and services that use covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system
- FAR rule took effect August 13, 2019

Part B

- Prohibits agencies from working with contractors that are ***using*** covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, *even if that use is unrelated to the contractor's federal business*
- FAR rule effective August 13, 2020

Section 889: Part B

X **DON'T** have to flow-down requirements to subcontractors/suppliers

- *But it seems that everyone is flowing it down in any event…*

✓ **DO** have to conduct a "reasonable inquiry" into products/services owned or provided to you by subcontractors/suppliers you use

X **DON'T** have to flow requirements to affiliates, parents and subsidiaries (for now)

- *Note: Part A requirements **DO** flow-down to subcontractors (FAR 52.204-25(e))

Section 889: DFARS Clauses

FAR

- Prohibition on Providing (Part A), *and* Use (Part B)
- Applies to certain "video surveillance" services not covered by the DFARS
- **Interim rule**

VS

DFARS

- Prohibition on Providing (Part A)
- Applies only to "covered missions"
- Applies to companies owned/controlled by the Russian Federation
- Final Rule

Section 889: DFARS Clauses (cont'd)

DFARS 252.204-7018	DFARS 252.204-7017	DFARS 252.204-7016
All ***contracts***	All ***solicitations***	All ***solicitations***
Contractors prohibited from ***providing*** to the DOD any equipment or services to carry out covered missions* that use covered defense telecommunications equipment or services ***as a substantial or essential component of any system***, or as a critical technology as part of any system. *"Covered Mission" = nuclear, missile defense, homeland defense	Certification: Offerors to represent whether it ***will/will not provide*** covered defense telecommunications equipment or services to the DOD ***in the performance of the specific contract/subcontract/ solicitation***.	Certification: Offerors must represent whether it ***does/does not provide*** covered defense telecommunications equipment or services to the DOD, ***generally, whether as a prime or subcontractor***.

Section 889: DFARS Clauses (cont'd)

- Section 1656 of the FY2018 NDAA has a broader scope than just Section 889
  - Broadly prohibits covered defense telecom equipment produced or provided by entities controlled by China **AND** Russian Federation
  - "Excluded Parties" from China & Russia should be listed in SAM.gov
- Could also implicate Section 1260H of the FY2021 NDAA, which identifies "Chinese Military Companies" doing business in the United States
  - Includes 60 companies, including Huawei

Section 889: Self-Certification

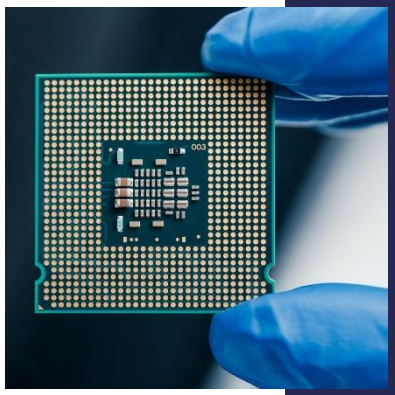
***Sierra7, Inc.; V3Gate, LLC* (B-421109, Jan. 2023)**

- VA used NASA SEWP contract to purchase personal computers, related equipment, and warranty support services
- VA accepted self-certification that products complied with Section 889
- Protesters argued that the VA did not investigate whether awardee's proposed Lenovo products complied with Section 889
  - Protesters alleged that awarded products were non-compliant, citing a 2019 DOD OIG report
- Decision suggests GAO/agencies will not question self-certification absent something in the proposal suggesting the certification was inaccurate

4. CHINESE SEMICONDUCTORS

Anti-Chinese Semiconductors

- Section 5949 of FY2023 NDAA
- Department of Commerce to create, in consultation with industry, a microelectronics traceability and diversification initiative to coordinate analysis of microelectronics supply chain vulnerabilities
- **Beginning in December 2027**, prohibits use of covered semiconductor product or services from a foreign country of concern
- "Covered semiconductor product or services" = semiconductor or a product that incorporates a semiconductor, or a service that utilizes such product that is designed, produced or provided by:
  - **Semiconductor Manufacturing International Corp. (SMIC)** (+ affiliates)
  - **ChangXin Memory Tech. (CXMT)** or **Yangtze Memory Tech. Corp. (YMTC)** (+ affiliates)
  - Any entity determined to be owned or controlled by, or otherwise connected to, the government of a **foreign country of concern**



Anti-Chinese Semiconductors (cont'd)

- Contractors who supply a Federal agency with electronic parts or products will be responsible for:
  - ✓**Certifying** to the non-use of covered semiconductor products or services in such parts or products;
  - ✓**Detecting and avoiding** the use or inclusion of such covered semiconductor products or services in such parts or products; and
  - ✓Any rework or corrective action that may be required to **remedy** the use or inclusion of such covered semiconductor products or services in such parts or products
- Contractors must notify the Government within 60 days of becoming aware, or having reason to suspect, that any product has been compromised
- 5-year timeline is designed to give industry time to plan ahead
  - Ramp-up domestic production of semiconductors
  - Ramp-down Chinese-origin products from supply chain

5. CHINESE FORCED LABOR

Chinese Forced Labor: Historically

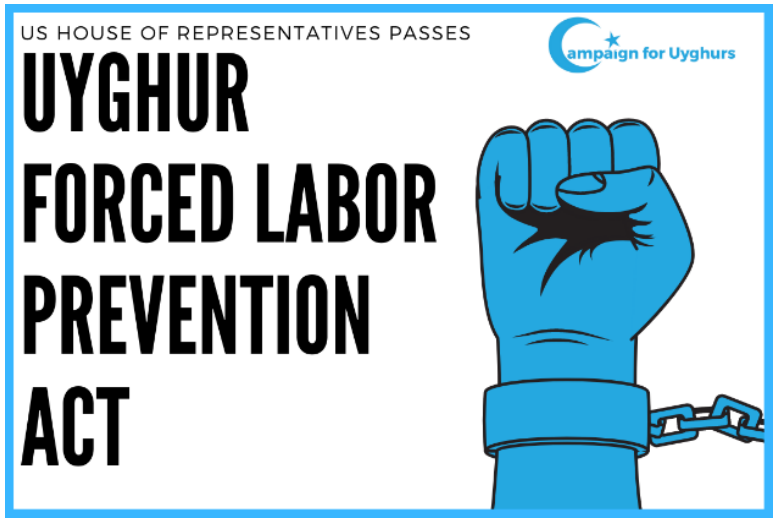
Pre-UFLPA (Uyghur Force Labor Prevention Act)

- U.S. Tariff Act Section 307 (19 U.S.C. 1307): Prohibits the importation of merchandise that has been mined, produced, or manufactured, wholly or in part, by forced labor
- "Reasonable care" standard for importers
- Consumptive demand exception

Chinese Forced Labor: Now

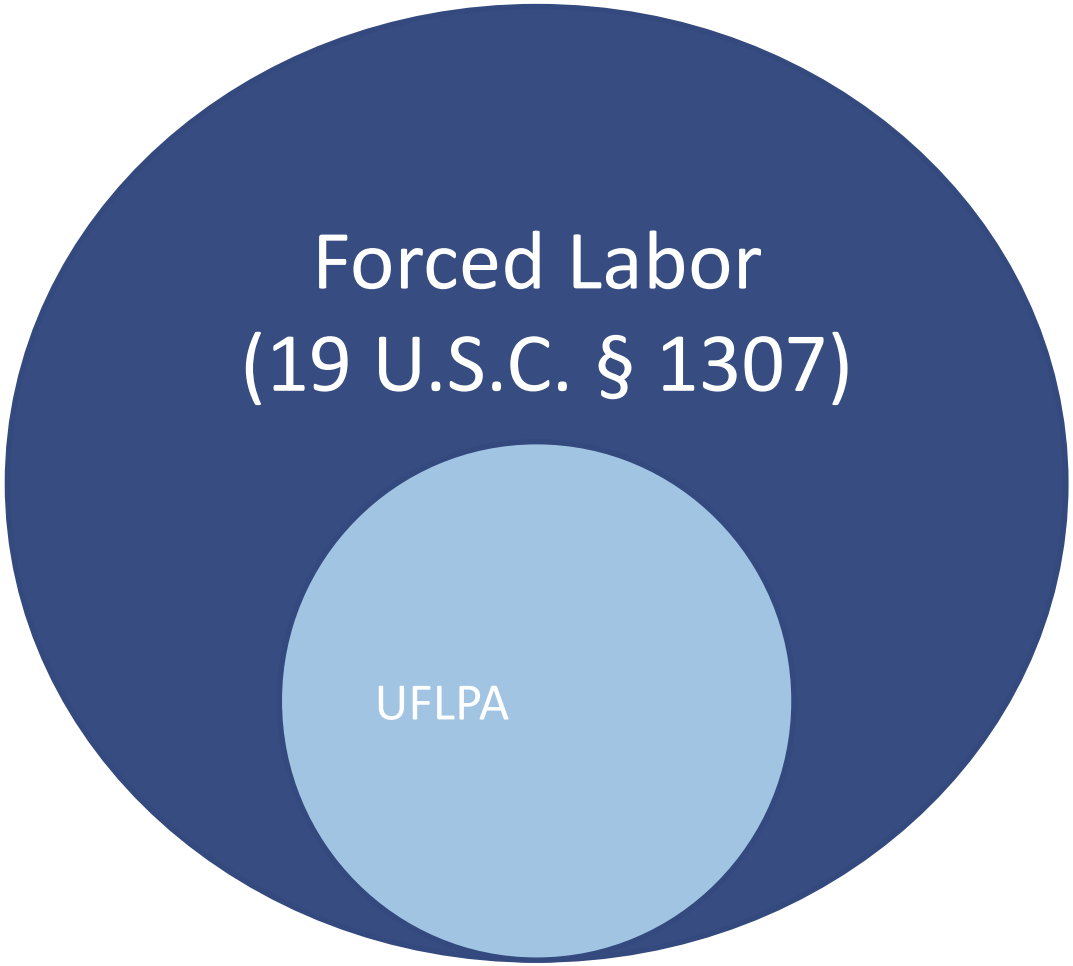
Post-UFLPA (Uyghur Forced Labor Prevention Act)

- Effective June 21, 2022
- Creation of **"rebuttable presumption"**
- From the Xinjiang Uyghur Autonomous Region (XUAR)
- "Guilty until proven innocent"
- No *de minimis* exception

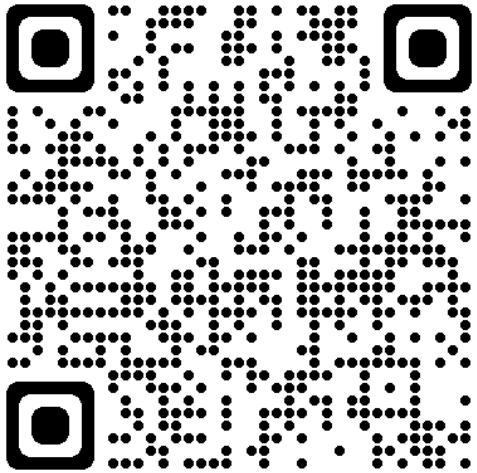


UFLPA Within the Context Of Forced Labor…

You want to be here…



Chinese Forced Labor: UFLPA Entity List



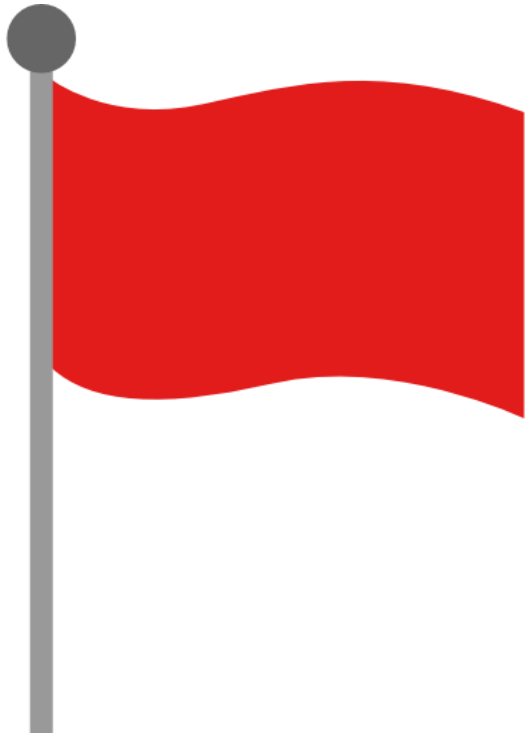
- Presumption that any entity on this list is involved in forced labor
  - (1) a list of entities in Xinjiang that mine, produce, or manufacture wholly or in part any goods, wares, articles, and merchandise with forced labor;
  - (2) a list of entities working with the government of Xinjiang involving forced labor of Uyghurs, Kazakhs, Kyrgyz, or members of other persecuted groups out of Xinjiang;
  - (3) a list of entities that exported products made by entities in lists 1 and 2 from China into the United States; and
  - (4) a list of facilities and entities, that source material from Xinjiang or from persons working with the government of Xinjiang or the Xinjiang Production and Construction Corps for purposes any government-labor scheme that uses forced labor.
- The list is expected to expand…

Chinese Forced Labor: XUAR

- UFLPA Region Alert Enhancement
  - Importers are required to report a valid postal code for cargo releases when the manufacturer's country of origin is China
  - Warning message will be issued when an XUAR zip code is provided
  - Possible risk of exclusion

Chinese Forced Labor: High Priority Industries

- UFLPA Targets
  - Polysilicon
    - Silica-based products
  - Tomatoes
  - Apparel
  - Cotton
- Recent Documents from U.S. Customs
  - Aluminum
  - PVC
- High Risk Areas
  - Artificial flowers, Christmas decorations, coal, fish, footwear, garments, gloves, hair products, nails, bricks, **electronics**, fireworks, textiles, toys



Chinese Forced Labor: Risk Assessment

Inputs of Risk

Identified Suppliers

Persecuted Minorities

Material, Product, or Industry

Geographical Origin

Working Conditions

Sources of Risk

UFLPA Entity List

Priority Sectors for Enforcement

Public data

CONCLUSION

Key Takeaways

- Complicated dance with China
  - We don't like them… but we kind of *do* like them
  - Tensions will likely continue to increase, with greater emphasis on Supply Chain Security
  - Continued monitoring of Chinese labor inputs
- Sanctions programs are likely to continue to shift – keep watching
  - Avoid: Cuba, Iran, North Korea, Syria, and sanctioned regions of Ukraine (and watch out for countries like Russia, Sudan, Myanmar, etc.)
  - Make sure that you are screening new contacts

Questions?

Sheppard Mullin Supply Chain Team

Lisa Mays
Associate
+1 714.424.8278 | Costa Mesa, CA.
lmays@sheppardmullin.com

David Gallacher
Partner
+1 202.747.1921 | Washington, D.C.
dgallacher@sheppardmullin.com