BSA/ AML and Sanctions Updates You Should Know:

Sept 15, 2023 | California Bankers Association 2023 Bankers Summit

Deborah S. Thoren-Peden | Partner
deborah.thorenpeden@pillsburylaw.com
+1.213.488.7320

Jacob Rivkin | Senior Manager
jacob.rivkin@crowe.com
+1.818.325.8659

This presentation does not constitute legal advice.

Agenda

1. Let’s Recap - What is the AML Act of 2020?
2. Corporate Transparency Act (CTA)
3. National Priorities
4. FinCEN Recent Updates & What Could Be Next
5. Sanctions and Exports Controls Updates

AML Act of 2020

- Passed on January 1, 2021, the FY2021 National Defense Authorization Act (NDAA) includes some of the largest revisions to the Bank Secrecy Act (BSA) and other Anti-Money Laundering (AML) regulations since 2001.
- Comprised of 4,500 pages of which approximately 200 pages are specifically related to AML/BSA and Countering the Financing of Terrorism (CFT).
- There are five key sections relating to BSA/AML regulations, which may impact an organization's compliance efforts.

The five sections of the AML Act of 2020 include:

1. Strengthening Treasury Financial Intelligence AML, and CFT Programs;
2. Modernizing the AML and CFT System;
3. Improving AML and CFT Communications, Oversight and Processes;
4. Establishing Beneficial Ownership ("BO") Information Reporting Requirements; and
5. Miscellaneous.

Corporate Transparency Act

What is the Corporate Transparency Act (CTA)

- The CTA establishes uniform beneficial ownership reporting requirements for corporations, limited liability companies, and other similar entities formed or registered to do business in the United States.
- The CTA authorizes FinCEN to collect that information and share it with authorized government authorities and financial institutions, subject to effective safeguards and controls.
- CTA effective date is January 1, 2024

Changing Beneficial Ownership Reporting Through the CTA

- Two notices from FinCEN so far on the implementation of the CTA:
  - September 29, 2022 – Final rule issuance
  - December 16, 2022 – Notice of Proposed Rulemaking regarding access to BOI and related safeguards
  - A third notice is expected, possibly to discuss the data receptacle (BOSS).

CTA Revising the 2016 CDD Rule

- The CTA requires that FinCEN revise portions of the 2016 CDD Rule within one year of the effective date of the CTA.
  - The 2016 CDD Rule is codified in 31 CFR 1010.230.
    - The general requirement for financial institutions to identify and verify the beneficial owners of legal entity customers under 31 CFR 1010.230(a) will remain.
    - The specific beneficial ownership identification and verification requirements under 31 CFR 1010.230(b) - (j) must be rescinded by FinCEN to make way for the CTA codified elsewhere.
- The CTA puts the beneficial ownership reporting responsibility on the reporting company itself rather than having the financial institution gather data during account opening.

Mapping the CDD Rule to the Corporate Transparency Act for Reporting Companies

1

Who Reports

- CDD – Natural person opening account on behalf of legal entity.
- CTA – Reporting company "agent".

2

What is Reported

- CDD – Control prong individual and ownership prong individual(s).
- CTA – Control prong individual (further defined), ownership prong individual(s), and agent certification.

3

Where is it Reported

- CDD – On Certification of Beneficial Ownership (COBO) form.
- CTA – Electronically within the Beneficial Ownership Secure System (BOSS) owned and operated by FinCEN.

4

When is it Reported

- CDD – At account opening.
- CTA – Within 30 calendar days of either the company's registration or public notice of the company's creation by the Secretary of State or similar office.

How the Corporate Transparency Act Impacts Financial Institutions (FI)

Responsibilities Change

- The CTA will relieve FI's from the burden of collecting and retaining BOI. Now collection and retention responsibility will reside with FinCEN, as the owner of BOSS, and the reporting company. However, FI's will still have the responsibility of determining applicable legal entity customers have completed a BOSS entry under the remaining portion of the CDD Rule codified at 31 CFR 1010.230(a).

FI's Process Change

- Onboarding and periodic reviews will have process changes.
- Training decks should be updated to reflect new processes.
- FIs must have a reporting company's consent to request BOI from BOSS.

FI's To-Do List

- FIs must develop and implement administrative, technical, and physical safeguards reasonably designed to protect BOI as a precondition for accessing BOI.
- Enroll associates completing BOI verification in the FinCEN developed online training. FinCEN expects FI BOSS system users to complete as a condition of creating and maintaining system accounts for access.
- Establish and maintain an auditable system of standardized records for requests.

CTA – FI Preparing for Implementation

- Update your AML Program / Policy.
- Since the CTA will be changing BOI responsibilities for FIs, changes to new customer onboarding and periodic review policies and procedures.
- BOSS system users should be identified, and training should begin as soon as the FinCEN online BOSS training is made available to ensure your institution has access.
- Establish a policy and plan for obtaining consent from potential and existing clients to validate beneficial ownership information in BOSS to comply with the portion of the CDD Rule that will remain intact.
- Prepare a plan for those reporting companies that are out of compliance, where no BOSS entry can be located (new and existing clients).
- Determine what you will do with legacy CDD Rule data; will it be used to compare against data in BOSS?
- Establish administrative, technical, and physical safeguards of BOI, and restrict access to appropriate persons.
- Establish and maintain an auditable system of standardized records for requests.

National Priorities

National Priorities Background

- The AML Act required FinCEN to issue a list of national priorities (Priorities) for addressing AML and CFT. On June 30, 2021 FinCEN issued the eight (8) Priorities, in no particular order.

- The Priorities do not amend BSA requirements, but the federal banking agencies plan to revise BSA regulations.
- FinCEN will issue regulations at a later date that will specify how FIs should incorporate these Priorities into their risk-based AML programs
- Banks and NBFIs are not required to incorporate the AML/CFT Priorities into their risk-based AML programs until the effective date of the final regulations.
- Banks and NBFIs can be forward-looking and may wish to start considering how they will incorporate the AML/CFT Priorities into their risk-based AML programs.

What are the Priorities?

- Corruption
- Cybercrime
- Terrorist Financing
- Fraud
- Transnational Criminal Organization Activity
- Drug Trafficking Organization Activity
- Human Trafficking and Human Smuggling
- Proliferation Financing

Corruption

- Corruption is typically defined as “abuse of entrusted power for private gain”.

- **Items to think about now:**
  - How does corruption specifically affect your organization?
  - Do you have an anti-bribery or anti-corruption policy?
  - Does employee training cover the topic of corruption?
  - Does your company have a PEP policy, procedure, approval process, and exit strategy that aligns with your risk tolerance?
  - Do you have the appropriate governance processes in place for policies and procedures?

Cybercrime

- Cybercrime threats against the US financial system, and other covered institutions is a strong concern of the US Treasury.

- **Items to think about now:**
  - Do you have strong network and infrastructure controls?
  - Are your employees, contractors, and vendors trained in phishing techniques, and other social engineering schemes?
  - Have you properly assessed the risk and threats related to cyberattacks?
  - Is sensitive data properly secured?
  - Do you maintain proper documentation of access control, onboarding and offboarding for system access, and periodic testing to confirm controls are working as intended?

Terrorist Financing

- Terrorism is evolving and is a relevant threat to the security of the USA. Cutting off financing to terrorist organizations can help derail vital operations, like recruitment, training, etc.

- **Items to think about now:**
  - Are the OFAC and sanctions screening models validated and tuned according to your risk-based approach and related OFAC / sanctions risk?
  - Do you conduct ongoing testing to verify third-party OFAC and sanctions screening list updates?
  - Have OFAC and sanctions red flags been incorporated into employee training programs?
  - Is your company properly filing thorough and timely SARs where applicable and notifying law enforcement when immediate notice is required?

Fraud

- Fraud, including bank fraud, provides the largest amount of illicit proceeds within the USA.

- **Items to think about now:**
  - Are applicable employees aware of the different types of fraud and most common scams and schemes?
  - Are your monitoring systems properly validated and tuned to identify common red flags for fraud?
  - Have these red flags been incorporated into employee training programs?
  - Are you properly filing thorough and timely SARs where applicable and notifying law enforcement when immediate notice is required?

Transnational Criminal Organization (TCO) Activity

- Transnational organized crime refers to organized crime that takes place in two or more countries.

- **Items to think about now:**
  - Are applicable employees aware of these types of organizations? Do they understand the risks and red flag indicators?
  - Have these risks and red flags been incorporated into employee training programs?
  - Is your CIP in line with regulatory expectations?
  - Is your KYC program asking the right questions and collecting the right information to truly understand your customers' expected activity?
  - Are you regularly refreshing your customers' profiles to confirm accurate information is on file?

Drug Trafficking Organization (DTO) Activity

- DTOs are a type of TCO that specialize in the drug market. Proceeds from illegal drugs are many times laundered through the USA, and the drugs affect American citizens directly.

- **Items to think about now:**
  - Is your organization aware of red flag indicators for drug trafficking activity, funnel accounts and TBML?
  - Are your monitoring systems properly validated and tuned to identify common red flags for drug trafficking activity, funnel accounts, and TBML?
  - Have these red flags been incorporated into employee training programs?
  - Do your due diligence programs consider private banking accounts held for non-US persons, and correspondent accounts maintained for foreign financial institutions?
  - Is your CIP in line with regulatory expectations?
  - Is your organization incorporating SAR terms for drug activity?

Human Trafficking and Human Smuggling

- Human trafficking exploits people against their will for gain, and human smuggling is the illegal transportation of individuals into foreign jurisdiction, typically for a fee.

- **Items to think about now:**
  - Does your organization understand the differences between human smuggling and human trafficking?
  - Are your monitoring systems properly validated and tuned to identify common red flags for human trafficking and human smuggling?
  - Have these red flags been incorporated into employee training programs?
  - Is your organization incorporating SAR terms for human smuggling / human trafficking activity?
  - Are questions regarding human trafficking and human smuggling incorporated as part of your due diligence process for applicable high-risk customer types that might also have an AML program (ex. MSBs, TPPPs etc.)?

Proliferation Financing

- These networks of individuals and entities seek to exploit the US financial system to move funds that will be used:
  1. to acquire weapons of mass destruction or delivery systems or their components; or
  2. in the furtherance of state-sponsored weapons programs, including the evasion of United Nations or US sanctions.

- **Items to think about now:**
  - Are you in compliance with required sanctions programs?
  - Are your sanctions screening models regularly validated?
  - Is your sanctions compliance program routinely audited by qualified third-party?
  - Do you bank or offer services to maritime, energy, or metals customers? Have you evaluated the due diligence in place to mitigate risk associated with these customers?
  - Do you have the appropriate controls in place for maritime industry clients?
  - Do your clients have appropriate sanctions programs in place?
  - Do you have a robust due diligence program to detect if your customers are operating near or in areas determined to be high-risk?

FinCEN's Spring 2023 Rulemaking Agenda

Projected Month	FinCEN's Plan
July 2023	• NPRM for section 6314 of AML Act and the AML Whistleblower Improvement Act
September 2023	• Final Rule for BOI access and safeguards and use of FinCEN identifiers.
November 2023	• Final Rule for section 6212: SAR Sharing Pilot Program
December 2023	• NPRM for section 6101(b): National Exam and Supervision Priorities • NPRM to revise existing CDD Rule

What can you do now to get prepared?

… Just START!

1. Stay Informed: Be aware of the potential changes coming.
2. Tell Those that Need to Know: Keep the Board and Senior Management informed.
3. Assess the Risk: Risk assessments continue to be a key first step for any action and control created.
4. Resources and References: Rely on credible sources and read the references!
5. Team Mentality: Consult with your business lines.

SANCTIONS UPDATE; EXPORT CONTROLS AND CFIUS

- Matt Rabinowitz of Pillsbury co-authored these slides.

Background on U.S. Sanctions

- U.S. Sanctions
  - Apply to activities by U.S. persons involving sanctioned parties or sanctioned countries
    - Has implications for financial transactions where U.S. banks are involved or US dollars are cleared through U.S. intermediary banks
    - Secondary sanctions exposure for activities by non-U.S. persons outside of U.S. sanctions jurisdiction
  - Comprehensive embargoes prohibit all or nearly all transactions in certain countries
    - General or specific licenses may allow certain activities in sanctioned countries
  - Additional restrictions on individually designated parties, with the scope varying depending on the designation (Specially Designated National, SSI List, etc.)

Background on U.S. Export Controls

- U.S. Export Controls
  - The Export Administration (EAR) broadly regulate exports, reexports, and transfers of "dual use" (military use and civil use) and commercial commodities, software and technology.
  - Impose specific export license requirements based on the item's export classification and destination country
  - Additional export license requirements for designated individuals and entities
    - Scope varies based on designation list (e.g., Entity List, Military End User List, etc.)
  - Items subject to the EAR:
    - All items in the U.S. or of U.S.-origin.
    - Certain Non-U.S. items:
      - Foreign-made items that incorporate U.S.-origin controlled content in excess of "de minimis" levels -- 25% for most destinations
      - Certain foreign-made items that are the "direct product" of certain controlled U.S.-origin technology or software

Background on the Russia and Belarus Sanctions Program

- In 2014, the United States and global allies issued sanctions against Russia after its invasion of the Crimea region of Ukraine.
- In response to Russia's invasion of Ukraine in 2022, the U.S. and global allies have coordinated global sanctions and export controls against Russia and Belarus.
- Scope of restrictions include:
  - Sanctions against Russian and Belarusian institutions and individuals, with a focus on Russian banks and Russian oligarchs;
  - Additional targeted sanctions against certain services, imports
  - Expanded export controls targeting lower-level controlled goods (oil refining equipment, semiconductors, mass market encryption, aviation)

U.S. Restricted Services

- Pursuant to EO 14071, on May 8, 2022, OFAC prohibited the export, reexport, sale, or supply, directly or indirectly, from the US, or by a U.S. person of the following services: **accounting, trust and corporate formation, and management consulting** to any person located in the Russian Federation.
  - **"Accounting services"** – includes services related to the measurement, processing, and transfer of financial data about economic entities.
  - **"Trust and corporate formation services"** – includes services related to assisting persons in forming or structuring legal persons, such as trusts and corporations; acting or arranging for other persons to act as directors, secretaries, administrative trustees, trust fiduciaries, registered agents, or nominee shareholders of legal persons; providing a registered office, business address, correspondence address, or administrative address for legal persons; and providing administrative services for trusts.
  - **"Management consulting services"** – includes services related to strategic advice; organizational and systems planning, evaluation, and selection; marketing objectives and policies; mergers, acquisitions, and organizational structure; staff augmentation and human resources policies and practices; and brand management.

UK and EU Restricted Services

- The UK and EU have imposed similar restrictions on services:
  - The UK has prohibited management consulting, accounting public relations services, **transactional legal, IT, engineering, auditing,** and **advertising services** to the government of Russia and persons, entities and bodies established in Russia. Transactional legal services cover certain commercial and transactional services.
  - The EU has prohibited accounting, auditing, statutory audit, bookkeeping and tax consulting services, business, trust advising, management consulting, on **architectural and engineering services, legal advisory services and IT consultancy services** to the government of Russia, as well as to legal persons, entities or bodies established in Russia.

Additional Restrictions from Other Jurisdictions

- Allied Countries
  - EU and UK restrictions against banks, entities and oligarchs have largely mirrored the U.S. sanctions, with some exceptions.
  - The EU and UK have emphasized that the next stage of sanctions will rely on enforcement.
  - Coordinated sanctions on Russia have come from an unprecedented number of countries, including Canada, Japan, Australia, South Korea, Singapore, Switzerland and Taiwan.
- Group of 7 Nations
  - G7 countries have committed to prevent Russia from accessing multilateral financial institutions such as the International Monetary Fund and the World Bank.
  - On September 2, 2022, the G7 announced the intention to impose a price cap on Russian origin oil. The price cap will prohibit services to maritime vessels transporting oil sold at a price above the cap. Details are still being formalized, but it is intended to go into place before December 5, 2022.

Society for Worldwide Interbank Financial Telecommunication (SWIFT)

- SWIFT is a private financial messaging service that allows transfer orders between banks around the world in more than 200 countries and territories.
- A number of Russian and Belarus banks have been delisted from SWIFT:
- Delisted banks are impacted not only in countries that apply sanctions to those banks, but in any jurisdiction where the bank ordinarily relies on SWIFT to interact with other banks.

U.S. Export Controls on Russia and Belarus

- All items on the Commerce Control List (CCL), *i.e.*, any Export Control Classification Number (ECCN) in Categories 0-9, are now controlled for Russia and Belarus.
- Includes a number of less sensitive items:
  - 3A991 semiconductors
  - 5A991 telecommunications equipment
  - 5A992 mass market items (e.g., mobile phones, laptops, etc.)
  - 9A991 commercial aircraft and related parts
- Selected EAR99 items are controlled for Russia and Belarus as well, included in Supplement 6 to Part 746.
- As of May 11, 2022, BIS has also imposed license requirements for a wide array of industrial items not otherwise specifically listed in the EAR, such as engines and building materials.
- There is a policy of denial for licenses.
- License exceptions may be available for certain items but are limited.

Countersanctions Measures (Russia)

- Russia has adopted a list of “unfriendly states” and imposed restrictions on their ability to repatriate funds and exit the market.
- In certain instances, the Russian government has targeted specific industries and companies with the primary goal of supporting and stabilizing the Russian economy at the expense of foreign investors.
- The Russian government has also designated individuals, including Western leaders and business executives.

What's Next?

- US Government and allies have made clear there will be more sanctions and export controls as the situation in Ukraine worsens
- Additional SDN/Entity List designations of individuals and companies
- Continue to restrict license exceptions in the EAR
- Prohibition on legal services from the U.S.?
- Sanctions on the Russian nuclear industry?

Due Diligence for Companies and Transactions

- KYC checks on parties, banks, vendors, business partners when dealing with transactions that may involve sanctioned parties, persons or products
- KYC checks can include identifying the UBOs for OFAC's 50% test and the EU's control test
- M&A transactions need to know if buying violation or unacceptable risk for exposure to sanctions or export controls violations
- Not all risks are the same so need to understand the purpose and scope of the sanctions if parties are on a sanctions-type list

Targeted export and import controls impacting supply chain, transactions and even IPOs

Expanded Use of List Based Controls Mainly Targeting China and Russia

- Export Control Lists
  - BIS Entity List
  - Military End Use Rule and Military End User List
  - FDP Footnote 1 Huawei Type restriction
  - FDP Footnote 4 restriction for 28 Chinese parties on the Entity List
- OFAC Sanctions Lists
  - SDN and the 50% rule
  - Sectoral Sanctions List (SSI)
  - Chinese Military-Industrial Complex Companies List
- Import Controls
  - Uyghur Forced Labor Prevention Act

Export Control Lists: BIS Entity List

- BIS list of names of foreign persons that are subject to specific license requirements for the export, reexport, and/or transfer (in-country) of items (commodities, software, and technology) subject to the EAR
  - List includes parties designated on national security or foreign policy grounds
  - Increasing focus on foreign policy issues, such as human rights violations and supply chain concerns
  - Independent of, and in addition to, license requirements otherwise imposed in the EAR
- Generally, BIS will impose a license requirement for all items subject to the EAR, including EAR99 items
- License applications are typically subject to a "presumption of denial"; however, BIS may call for a "case by case" review of certain ECCNs

Military End User/Military End Use (MEU) Rule

- License requirement for exports, reexports, or transfers of certain items if the exporter has "knowledge" that the item is intended for a military end use or a military end user in **China, Russia, Belarus Venezuela, or Myanmar (Burma)**.
  - Scope varies depending on the specific MEU type rule
- Covers "military end user" and "military intelligence end users" depending on the rule.
  - Traditional foreign military and related organizations (e.g., military, national guard, national police, etc.); and
  - Any other end user whose activities are intended to support 'military end uses'
- BIS published an MEU list but not exhaustive

Military End User/End Use Rules

	MEU Rule	Expanded MEU Rule (Russia and Belarus)	Military Intelligence End-Use Rule
Items	Any item subject to the EAR listed in Supplement No. 2 to Part 744 (e.g., 3A991 chips, 4A994 computers, 5A991 telecommunications equipment, 5A992 mass market items, 9A991 aircraft, etc.)	Any item subject to the EAR	Any item subject to the EAR
Destination	"military end user" or for a "military end use" in China, Venezuela, Myanmar (Burma), or Cambodia	"military end user" or for a "military end use" in Russia or Belarus	'military-intelligence end user' or for a 'military-intelligence end use' in China, Russia, Belarus, Myanmar (Burma), Venezuela, Cambodia, or embargoed destinations (*i.e.,* Iran, North Korea, Syria, or Cuba)
Definitions	"Military end user" is defined as: • Traditional foreign military and related organizations (e.g., military, national guard, national police, etc.); and • Any other end user whose activities are intended to support 'military end uses' "Military end use" is defined as: • incorporation into a military item described on the U.S. Munitions List (USML); • incorporation into items classified under ECCNs ending in "A018" or under "600 series" ECCNs; • or any item that supports or contributes to the operation, installation, maintenance, repair, overhaul, refurbishing, "development," or "production," of military items described above	"military end user" and "military end use" are defined the same as under the traditional MEU rule.	"Military-intelligence end user" is defined as: intelligence or reconnaissance organization of the armed services (army, navy, marine, air force, or coast guard); or national guard "Military-intelligence end use" is defined as: design, development, production, use, operation, installation, maintenance, repair, overhaul, or refurbishing of, or incorporation into, USML items or items classified under A018 ECCN or 600 series ECCNs when intended to support the functions of a MIEU

MEU Rule Takeaways

- Imposes due diligence obligations on parties to determine whether their end users are military end users, or whether their products would otherwise be used for a military end use.
- Has resulted in heightened scrutiny on Russian, Belarusian, and Chinese companies in particular, as exporters seek to determine whether a company is a military end user, supports any military end uses, or does business with military end users.
- Different companies will have different risk-based approaches. Exporters will conduct due diligence, including sending, to determine if an entity is a “military end user” and whether a transaction invquestionnaires/certificationsolves a “military end use.”
- U.S. suppliers (and non-U.S. suppliers providing items subject to the EAR) should conduct an MEU assessment of end users in China, Russia, Belarus, Myanmar (Burma), and Venezuela.

Sanctions - Specially Designated Nationals (SDN) List

- List of individuals and entities who are “blocked”
  - U.S. persons prohibited from doing business with a person on the SDN List
  - SDN property interests that enter possession or control of U.S. person must be blocked
  - Effectively prohibits dealing in U.S. dollars as U.S. banks clearing the funds must freeze the transaction and report to OFAC
  - Designation apples to any entity owned 50% or more by SDN (OFAC’s 50% Rule)
- For example, many Russian banks have been added to OFAC’s SDN List, including: Sberbank, Alfa Bank, VTB, VEB, PSB, Otkritie, Sovcombank, Novikombank and Moscow Industrial Bank.
- In addition to full blocking sanctions, OFAC also issued narrower restrictions with specified financial institutions via directives.

Chinese Military-Industrial Complex Companies List

- **E.O. 13959 (issued Nov. 2020) as amended by E.O. 14032 (issued June 3, 2021)** – prohibits U.S. persons from engaging in the purchase or sale of publicly traded securities of designated entities.
  - E.O. 14032 expanded the scope of potentially designated parties to include parties determined to operate in China's defense or surveillance technology sector, defined as Chinese Military-Industrial Complex Companies ("CMICs").
  - The non-SDN CMIC List replaced the previous Communist Chinese Military Companies ("CCMC") List under E.O. 13959.
  - Restrictions take effect 60 days after identification on the CMIC List. U.S. persons have 365 days from the effective date of any listing to divest any CMIC-restricted securities.
  - Designation on the CMIC List does not necessarily mean a party is an MEU subject to license requirements under the EAR; however, it is a red flag triggering further due diligence.

List Based Sanction Takeaways

- Need to screen parties to the transactions, owners and key business partners against the various lists
- Not all lists are the same – need to distinguish between
  - Export control-based lists - restrictions dealing with products, software and technology and
  - Sanctions-based list - restrictions impacting transactions with parties on sanctions list
- Some restrictions can impact IPOs and may require special sanctions and export control expert opinions on impact
  - Can include dealing with parties (key suppliers, vendors, etc.) on the list even if company being involved in IPO is not on the list

Import Prohibitions: Forced Labor

- **Section 307 of the Tariff Act (19 USC 1307)** bans the import of goods produced "wholly or in part" by convict labor or forced labor
  - ***Interpreted to cover forced labor "at any tier of their supply chain, down to every input into the products"***
  - Largely enforced by "Withhold Release Orders (WROs)"
- Effective June 21, 2022, the (UFLPA) specifically targets the Xinjiang Uyghur Autonomous Region **Uyghur Forced Labor Prevention Act** of the People's Republic of China (XUAR).
  - All goods from XUAR are now presumed to be made with forced labor and banned from import
  - Also targets goods from identified entities (Entity List) both within and outside XUAR
  - Imposes a "clear and convincing" evidence standard for importers to overcome the presumption, similar to North Korea forced labor rebuttal standard per CAATSA – 22 USC 9241a

Forced Labor: Uyghur Forced Labor Prevention Act Guidance and Resources

- The Forced Labor Enforcement Task Force published the "Strategy to Prevent the Importation of Goods Mined, Produced, or Manufactured with Forced Labor in the People's Republic of China" on June 17.
  - This included the initial UFLPA Entity List and guidance for importers on due diligence, effective supply chain tracing, and supply chain management measures.
- Custom and Border Protection's Operational Guidance, published June 13, outlined the standards importers must comply with under UFLPA.
  - It clarified that if an importer believes that its importation has been wrongfully detained under the UFLPA, the importer may submit detailed documentation to prove that the goods and its components were produced outside of the XUAR.
  - Alternatively, it outlines how an importer may attempt to overcome the rebuttable presumption and the types of evidence importers may submit.
  - It established there is no de minimis exception.

Fallout of UFLPA Implementation

- Detentions have been reported, including extensive detentions of solar panel materials.
  - However, imports from the region are generally down.
- Importers have filed “applicability reviews” with CBP, which argue that the UFLPA should not apply to their materials under the CBP Operational Guidance.
- BIS has formally published the UFLPA Entity List, and will continue to add entities to the list.

Foreign Investment Restrictions

CFIUS Overview

- The Committee on Foreign Investment in the United States ("CFIUS") is an interagency committee led by the Department of Treasury, and the heads of the following departments and offices are members of CFIUS: Department of Justice; Department of Homeland Security; Department of Commerce; Department of Defense; Department of State; Department of Energy; Office of the U.S. Trade Representative; and Office of Science & Technology Policy. CFIUS is authorized to block "covered transactions" (either before or after close) or impose measures to mitigate any threats to U.S. national security.
- Reviews "covered transactions" that could result in control of a U.S. business by a foreign person.

CFIUS Overview

- CFIUS is authorized to block “covered transactions” (either before or after close) or impose measures to mitigate any threats to U.S. national security.
- Focused on national security (i.e., military) concerns but the interpretation of national security has evolved over the years to encompass broader national interests (e.g., economic security) and strategic threats (e.g., China).

Determining Whether There Is a "Covered Transaction"

- Any transaction which could result in "control "of a "U.S. business" by a foreign person.
  - U.S. business
    - Any entity engaged in U.S. interstate commerce
    - Covered transactions can include asset acquisitions
  - Control
    - Any arrangement that allows a foreign person to determine, direct or decide important matters affecting a U.S. business
- Non-control covered investments
  - Investment in any "TID US Business" that provides the foreign person with any of the following:
    - Board seat or Board observer;
    - Access to material non-public technical information (excluding financial information); or
    - Any involvement in the company's substantive decision-making
- Covered real estate transactions

TID U.S. Business

- **“TID U.S. Businesses” (Critical Technologies, Critical Infrastructure, and Sensitive Personal Data)**
- U.S. business that:
  - Owns, operates, manufactures, supplies, or services critical infrastructure;
  - Produces, designs, tests, manufactures, fabricates, or develops one or more critical technologies; or
  - Maintains or collects sensitive personal data of U.S. citizens that may be exploited in a manner that threatens national security

Critical Technologies

- **Critical Technologies** include:
  - Defense articles or defense services included on the United States Munitions List (USML)
  - Items on the Commerce Control List (CCL) beyond Anti-Terrorism (AT) controls
  - Nuclear items covered by 10 CFR 810 and 10 CFR 110
  - Select agents and toxins
- **Emerging and foundational technologies** controlled pursuant to section 1758 of the Export Control Reform Act of 2018.
  - Note no broad-based rule expected to control all technologies in certain sectors (e.g., AI, quantum computing, etc.). Rather, targeted rulemakings controlling specific technologies raising national security concerns

Executive Order Outlining Additional National Security Considerations for CFIUS

- E.O. 14083 (issued Sept. 15, 2022) highlights national security factors that tie into the Biden Administration's national security priorities
- Enumerates sectors in which supply chain resiliency and U.S. technological leadership face increased risk — including microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy, climate adaptation technologies, and critical materials.
- Directs the Committee to consider five specific factors in evaluating covered transactions:
  - Supply chains
  - Technological leadership in certain fields
  - Investment trends
  - Cybersecurity
  - Sensitive personal data

Critical Infrastructure

- **Critical Infrastructure** is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems or assets would have a debilitating impact on national security."
  - Only a non-controlling foreign investment in a U.S. business that **performs one of the specified "functions"** with respect to the corresponding **type of critical infrastructure** qualifies as a critical infrastructure covered investment.
  - Appendix outlines **28 categories** of critical infrastructure and their related "functions"

Sensitive Personal Data

- **Sensitive Personal Data** is defined as "identifiable data" falling into certain categories that is maintained or collected by a U.S. business that:
  - "Targets or tailors" its products or services to sensitive U.S. Government personnel or contractors
  - Has maintained or collected such data on greater than one million individuals; or
  - Has a demonstrated business objective to maintain or collect such data on greater than one million individuals and such data is an integrated part of U.S. business's primary products or services

Mandatory vs. Voluntary Filings

- Mandatory Filings
  - Control or non-control investment in a critical technology company for which an export license would be required in connection with the foreign acquirer
  - "Substantial interest" investments by foreign government in TID U.S. Businesses
    - 25% or greater voting interest (direct/indirect) by a foreign person in a TID U.S. Business
    - 49% or greater voting interest (direct/indirect) by a foreign government in a foreign person
- Voluntary Filings
  - Any foreign person acquiring control over any US business (traditional CFIUS rules)
  - Non-control investments in TID U.S. Businesses not covered by mandatory filings

Mandatory Filings – Critical Technology

- **Mandatory** filing requirement for control transaction or covered investment in:
  - US business that produces, designs, tests, manufactures, fabricates, or develops certain **critical technologies**, and where
  - A "U.S. regulatory authorization" would be required to export the critical technology to any of the foreign parties to a transaction. This includes:
    - A license or other approval issued by the Department of State under the International Traffic in Arms Regulations (ITAR);
    - A license from the Department of Commerce under the Export Administration Regulations (EAR);
    - A specific or general authorization required from the Department of Energy pursuant to 10 CFR Part 810; or
    - A specific license from the Nuclear Regulatory Commission pursuant to 10 CFR Part 110.
- Applies to acquiring entity and 25% or more owners
  - Includes both intermediate parent companies as well as ultimate beneficial owners that hold a 25% or greater interest.

Potential for Outbound Investment Review

- National Critical Capabilities Defense Act (NCCDA) - Proposed bill that would establish a new, expansive outbound "CFIUS-like" review mechanism for investments and other transactions involving "countries of concern" (China, Russia, etc.). Bipartison bill reintroduced to Congress in May, 2023.
- "Covered activities" include:
  - Developing or moving a national critical capability to or in a country of concern;
  - Technology transfer that supports a national critical capability by an entity of concern or in a country of concern; or
  - Outbound investment to enhance a national critical capability for an entity of concern or a country of concern.

National Critical Capabilities Defense Act (NCCDA)

- "National critical capabilities" tied to key supply chains such as:
  - semiconductor manufacturing materials,
  - large capacity batteries,
  - critical minerals and materials,
  - pharmaceuticals and active pharmaceutical ingredients, and
  - "critical and emerging technologies," such as artificial intelligence, bioeconomy, and quantum information science and technology.
- Mandatory filing requirement to Committee who could impose mitigation (including disinvestment) if transaction poses unacceptable security risk
- Likely challenges by some industry groups
- Biden Administration could consider issuing an Executive Order implementing similar framework.

Expected Trends

- Significant increase in review and enforcement involving “non notified transactions”
  - Could include situations where foreign person transferring previously acquired US business to a new foreign person
  - Be aware of press releases and other announcements (e.g., SEC filings)
- Continued focus/scrutiny on specific countries of concern such as China and Russia, as well as other state-owned enterprises
- Continued focus on cases involving personal data in particular
- Potential use of voluntary declarations for quicker timelines
- Parties to continue to use creative methods for closing transactions
- Multilateral engagement across similar investment schemes in partner countries
- Potential implementation of an outbound investment restriction

Thank You!