Association of Corporate Counsel (ACC) San Francisco Bay Area Presentation

Updates on Federal Contracting and Trade Control Laws: Issues for Doing Business with the US Government and with China

March 3, 2022

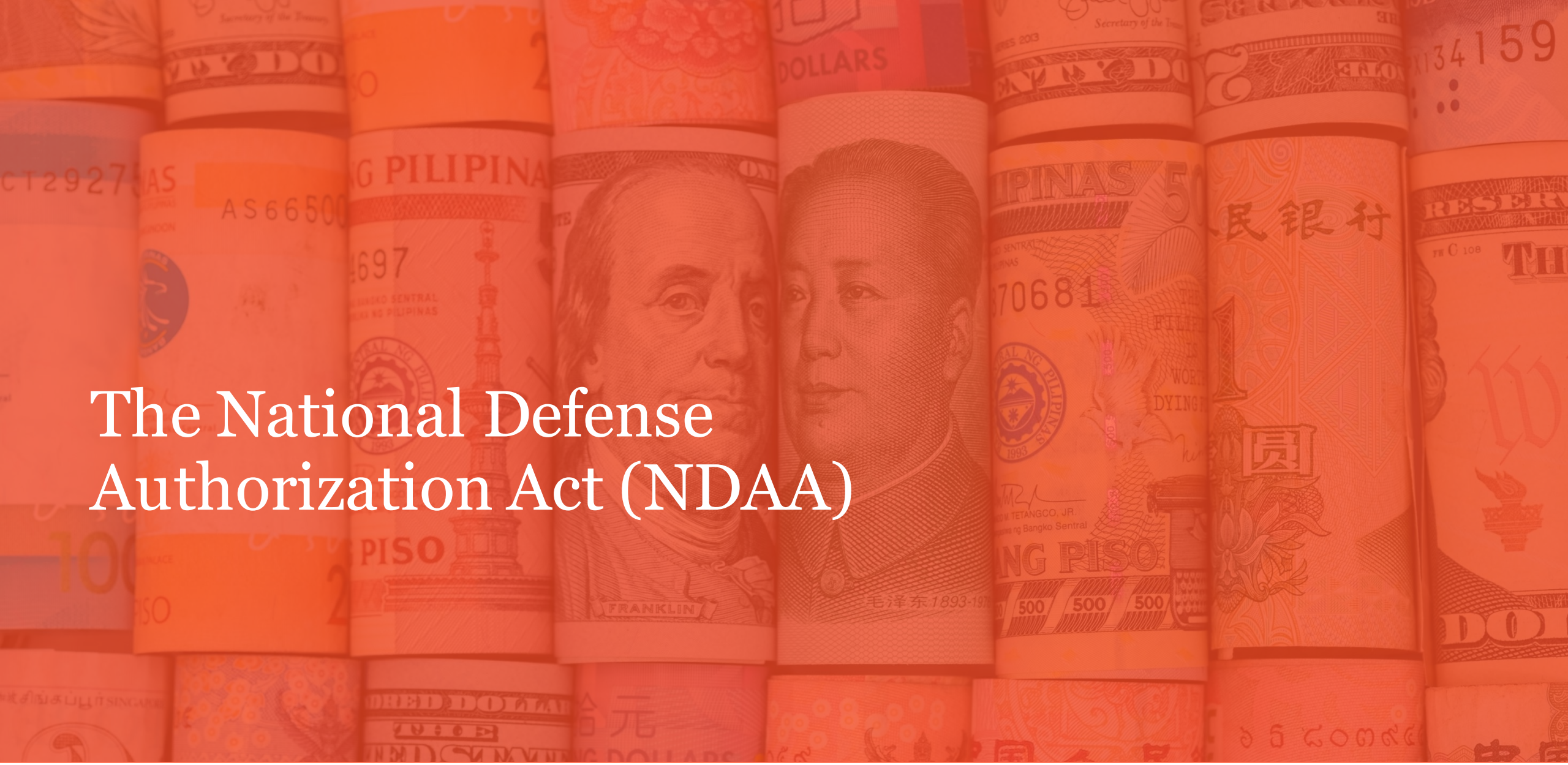
Christian C. Davis
Partner
Washington, D.C.

Scott M. Heimberg
Partner
Washington, D.C.

Akin Gump
STRAUSS HAUER & FELD LLP

AGENDA

- The National Defense Authorization Act (NDAA)
- Supply Chain
- Buy American Act (BAA)
- Export Controls
- Sanctions
- Committee on Foreign Investment in the United States (CFIUS)
- Information & Communications Technology and Services (ICTS)
- Outbound Investment Screening?



The National Defense Authorization Act (NDAA)

Akin Gump
STRAUSS HAUER & FELD LLP

What's New in NDAA 2022

- National Defense Authorization Act (NDAA) for FY 2022
  - Signed into law on December 27, 2021
  - Policy direction
    - Other Transaction Authority (OTA)
    - Small Business Matters
    - Sourcing and Supply Chain Security.
  - Cyber Security Provisions
    - Ransomware
    - Incident Responses
    - Controlled Unclassified Information (CUI)
    - Cybersecurity Maturity Model Certification (CMMC)
    - Procurement of Products and Services
    - PPP's
    - Critical Infrastructure.

NDAA FY 2022 OTAs

Title VIII Subtitle C Provisions Relating to Other Transaction Authority Further Encouraging Use of Other Transaction Authoritys (OTAs).

- In order to encourage more use of OTAs NDAA removes the requirement for The United States Department of Defense (DoD) to implement regulations before exercising research OTA authority.
- Authorizes the awarding of contracts and OTAs as “prizes” for advanced technology achievement.
- Authorizes a pilot program for award of OTAs for systems engineering and requires the Defense Innovation Unit and The Defense Advanced Research Projects Agency (DARPA) to award at least two OTAs, contracts or projects.
- Requires reports on the current use of OTAs by DoD to defense committees of Congress.
- Requires the collecting and publicizing of data on OTAs.

Other Transaction Authority

- So what is an OTA?
- Federal agency statutory authority to execute an agreement for a product or service without a standard format or required terms and conditions.

  > "The Secretary of Defense and the Secretary of each military department may enter into transactions (other than contracts, cooperative agreements, and grants) under the authority of this subsection in carrying out basic, applied, and advanced research projects."

- Not a contract, grant, cooperative agreement, or cooperative research and development agreement.
- Designed to allow the agency to tailor the OTA to meet specific situations.
  - No required intellectual property protections.
  - No Federal Acquisition Regulation.
  - No Cost Accounting Standards.

Laws/Regulations That Do Not Apply to OTA's

- Competition in Contracting
- Bayh Dole (relating to intellectual property rights)
- Small Business
- Domestic Preference Rules
- FAR/DFAR
- Truthful Cost or Pricing Data Act (TINA)
- Cost Accounting Standards.

NDAA FY 2022 Small Business

- Accelerated payments available to prime contractors, if agree to flow down to small business subcontractors.
- Extends pilot programs for streamlining awards for innovative technology projects to small businesses.
- Requires DoD to report on unfunded priorities relating to Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) projects.
- Requires DoD to collect data on funding and topics for Phase III awards under SBIR and STTR programs.

NDAA FY 2022 Sourcing and Supply Chain

- NDAA includes provisions to strengthen and secure key industrial bases in both the United States and the national industrial and technology base (NTIB) -- Australia, Canada and the United Kingdom.
- Focus on supporting domestic manufacturing and workers.
- ***Domestic Preferences – Shining light on waivers and violations.***
- Section 808 requires DoD to brief Congressional defense committees no later than 180 days on the extent to which information relating to the use of domestic procurement waivers by DoD is publicly available.
- Section 809 requires DoD to annually report violations of the Buy American Act, Berry Amendment or Specialty Metals statute to the Congressional defense committees beginning in 2023 and continuing through 2025.

NDAA FY 2022 Sourcing and Supply Chain Security

Supply Chain Security

- Section 841 requires DoD to develop the capability to map supply chains and assess supply chain risks for major end items (by business sector, vendor, program, part and other metrics) (addressing issues identified in the House Defense Supply Chain Task Force June 2021 report).
- Section 842 expands FY2021 NDAA § 849 list of high priority goods and services for DoD analyses, recommendations and actions.
  - beef products, molybdenum, optical transmission equipment (including fiber cable), armor on tactical ground vehicles, graphite processing and advanced AC-DC power converters.
- Section 847 directs DoD to develop and implement a plan to
  - (1) reduce reliance of the United States on services, supplies, or materials obtained from sources in geographic areas controlled by **North Korea, China, Russia or Iran.**
  - (2) mitigate the risks to national security and the defense supply chain related to relying on these nations' sources for services, supplies or materials to meet critical defense requirements.

NDAA FY 2022 Sourcing and Supply Chain Security

- Section 848 prohibits DoD from procuring any products mined, produced or manufactured, wholly or in part, by forced labor from **Xinjiang Uyghur Autonomous Region of China** (XUAR) or from an entity that has used labor from within or transferred from XUAR as part of a "poverty alleviation" or "pairing assistance" program.
  - Within 90 days of the enactment of the FY2022 NDAA, DoD must issue rules to require **certifications** from offerors for Defense contracts addressing this prohibition.
- Section 851 amends 10 U.S.C. § 2533d, which prohibits DoD from acquiring certain printed circuit boards from China, Russia, Iran or North Korea to, among other changes, **push the effective date** of these restrictions from January 1, 2023 to January 1, 2027.
- Section 855 requires covered entities to disclose to DoD if the entity **employs one or more individuals who will perform work in the People's Republic of China (PRC)** on a covered contract when the entity submits a bid or proposal for such covered contract. This Section takes effect on July 1, 2022.
  - "Covered entity" means any corporation, company, LLC, LP, business trust or association (including any subsidiary) performing work on a covered contract in PRC, including by leasing or owning real property used in performance of the covered contract in the PRC.
  - "Covered contract" means any DoD contract or subcontract with **a value greater than $5M**, **excluding commercial products or services**.

NDAA FY 2022 Sourcing and Supply Chain Security

- Section 5502 requires DoD to develop, within 30 days, a list of covered contractors with respect to which DoD should seek to avoid entering into contracts.
  - A "covered contractor" is a provider of **telecommunications, telecommunications equipment or IT equipment that has knowingly assisted or facilitated a cyber attack** or conducted surveillance against
    - (1) the United States by or on behalf of any government or persons associated with such government listed as a cyber threat actor in the Intelligence Community's 2017 assessment of worldwide threats to the United States; or
    - (2) individuals for the purposes of suppressing dissent or intimidating critics on behalf of a country included in the annual country reports on human rights practices for systematic acts of political repression. DoD is to develop the list in consultation with the Director for National Intelligence and other agencies and then must maintain and update the list as frequently as appropriate.

In addition to the above provisions, the FY2022 NDAA also includes specific sourcing restrictions at §§ 802, 816, 843, 854 and 1411, and additional supply chain analysis and authorities at §§ 844 and 1411.

Previous Supply Chain Security Actions

- Tighter Cyber Security.
  - Standards for handling Controlled Unclassified Information (CUI) to protect against advanced persistent threats DFARS 7012 clause.
  - CMMC.
- Exclusion of Certain Non-US suppliers.
  - Hardware, software and services from Kaspersky Labs.
  - Banning use of telecom and security camera equipment from Huawei, ZTE and other Chinese manufacturers.
- Reporting of Counterfeit Parts.
  - The Federal Acquisition Regulation (FAR) requirements to suspected counterfeit parts to the Government Industry Exchange Program.
- Creation of a Supply Chain and Counterintelligence Risk Management Task Force in 2020.
- Establishment of disclosure obligations where there is a risk of foreign-government influence over products and services.
- Evaluation of contractors based on ability to protect supply chain.

NDAA FY 2022 Cyber Security

- Ransomware – DoD to conduct assessment of ability to defend against ransomware attacks and make recommendations on deterrence by July 2022.
- Incident Responses -- Cybersecurity and Infrastructure Security Agency update and evaluate National Cyber Incident Response Plan and perform model exercises.
- CUI
  - Publish a report on
    - Whether DoD is properly marking/identifying CUI
    - When is commercial information CUI
    - Examples of information that is and is not CUI.
- Cybersecurity Maturity Model Certification (CMMC).
  - Report on the implementation of CMMC Version 2.
  - Report on the impact of CMMC on small business.

- Purchase of Cybersecurity Products.
  - DoD must by the end of the year designate an executive agent for enterprise-wide procurement of cyber data products and services.
  - DoD components will be prohibited from independently procuring these products after July 2023.

NDAA FY 2022 Cyber

- Public Private Partnerships – Cyber Command to establish a process to partner with private sector IT and Cyber Security companies to develop methods to fight “malicious cyber actors”.
- Strengthen Critical Infrastructure against cyber threats like the Colonial Pipeline ransomware attack.
  - Cybersecurity and Infrastructure Security Agency (CISA) to identify and mitigate cybersecurity threats to industrial control systems.
  - Report to Congress on efforts.
  - Establish CyberSentry program providing continuous monitoring and detection of cyber risks to owners and operators of critical infrastructure.
    - Sharing of intelligence and advising on mitigation measures.

Future for Protection of US Information and Communication Technology and Services (ICT)

- Last week, the Commerce Department and Department of Homeland Security issued a report assessing the state of and addressing vulnerabilities in the U.S. Information and Communication Technology and Services (ICT) supply chain.
  - Called for more domestic manufacturing incentives and new Buy American policies.
  - Identified structural vulnerabilities throughout the ICT supply chain, including
    - A lack of a domestic ecosystem for many segments of ICT production.
    - Overreliance on single-source and single-region suppliers.
    - Difficulty in maintaining product integrity due to complex supply chains.

- The Report called for the revitalizing the U.S. ICT manufacturing base through long-term investments.
  - The Creating Helpful Incentives to Produce Semiconductors in America Act (CHIPS Act).
  - Title III of the Defense Production Act support the production of key ICT products, like printed circuit boards, the report says.

Supply Chain

Akin Gump
STRAUSS HAUER & FELD LLP

Funding for Technology Supply Chain

- The CHIPS Act, enacted on Jan. 1, 2021, authorized the creation of incentive programs to spur domestic semiconductor manufacturing.

  Senate appropriated $52 billion to fund the CHIPS Act in the U.S. Innovation and Competition Act (USICA).

  The House earlier this month included similar funding in its America COMPETES Act.

  Congress is in the conference process and is expected to reconcile the two bills shortly.

- The Defense Production Act Title III program to expand domestic sources for critical technology items deemed essential to national security.

  Subsidies

  loans

  loan guarantees

  purchase commitments.

Recommendations for Supply Chain Office

- Creation of a supply chain office

  "to identify, monitor, and address supply chain vulnerabilities and partner with industry, labor, and other public and private stakeholders to strengthen resilience throughout the ICT industry."

- Both USICA and the America COMPETES Act would establish such an office within Commerce (with the latter authorizing $45 billion for it).

- Creation of an "Assured Supplier Program" aimed at connecting the federal government and critical sectors.

  Focus on ensuring the government can obtain products like printed circuit boards and semiconductors.

  Federal agencies that procure ICT for sensitive equipment should consider a preference for vendors.

  Participate in a voluntary qualified bidder or manufacturer program to

    assess their qualifications

    assurance of the reliability, integrity and security of their products.

Supply Chain Risk Management Best Practices

Executive Level Commitment

- Buy-In from Stakeholders
- Communication and Information Sharing
- Training and Awareness
- Policies and Processes.

Identify Critical Assets

- Implement Asset Management
- Prioritize Critical Systems, Networks and Information
- Be Vigilant for Indicators of Compromise.

Manage Third Party Risk

- Conduct Risk-Based Due Diligence on Suppliers
- Incorporate Security Requirements and certifications into subcontracts and supply agreements
- Monitor Supplier Compliance
- Implement Risk Mitigation Measures.

Continuous Improvement

- Monitor Effectiveness and Update as Needed.

Buy American Act (BAA)

What's Happening with the Buy American Act

- Several Executive Orders over the last four years emphasizing Buy American, including recent order by President Biden on Made in America.
- U.S. preference to buy domestic products is set out in the Buy American Act of 1933 (BAA) and FAR.
- BAA applies to "end products" purchased by the federal government.
- Two-part test:
  - Manufactured in the U.S.
  - The cost of U.S.-manufactured components must exceed 55 percent of the total cost of the components (95 percent for domestic iron or steel).
- Components are those items directly incorporated into the end product.
- No component test for Commercial Off the Shelf (COTS) items.
  - Note that the COTS waiver does not apply to iron and steel.

BAA Price Preference and Content

- Current Price Preference:
  - 20 percent/30 percent evaluation factor on civilian contracts -- raised by regulation on January 21, 2021, from 6 percent/12 percent.
  - 50 percent evaluation factor on DoD contracts.
- Current Domestic Content Requirement:
  - The cost of U.S.-manufactured components must exceed 55 percent of the total cost of the component cost (95 percent for domestic iron or steel).
  - Raised from 50 percent to 55 percent and 50 percent to 95 percent for domestic iron or steel on January 21, 2021, based on a Trump Executive Order (EO).

GSA Schedule – TAA Compliance

- BAA waived by international trade agreements as implemented by the Trade Agreements Act (TAA) and included in the Federal Acquisition Regulation.
  - TAA implements numerous multilateral and bilateral international trade agreements.
  - **The TAA applies to all GSA and VA Schedule contracts (unless otherwise stated in the solicitation or contract).**
  - The TAA limits the country of origin for end products sold to the U.S. government to U.S. end products or Designated Country end products.
  - Prohibits acquisitions of products made in countries other than the U.S. or designated countries (e.g., end products from China or India are prohibited).

Trade Agreements Act Exemption

- **U.S.-made end product** means an article that is mined, produced or manufactured in the United States, or that is substantially transformed in the United States.
- **Designated Country end product** means an article that
  - (1) Is wholly the growth, product or manufacture of a WTO GPA country; or
  - (2) In the case of an article that consists in whole or in part of materials from another country, has been substantially transformed in a designated country.
- **The TAA allows acquisitions of end products made in designated countries as if they were domestic – No BAA U.S. domestic content or price preferences are applied to these end products.**
- Designated Countries include WTO countries and other trading partners:
  - EU countries, South Korea, Japan, Canada and Mexico.

Trade Agreements Act Exemption

- Key consideration is what products are considered to be **"substantially transformed"** in the designated country.
  - Test is whether the product was subject to a manufacturing process in the country which results in a new and different article of commerce, with a new name, character or use.
- Factors to consider:
  - The complexity of the process.
  - The technical skill involved in the process.
  - The expense or value added by the process.
  - The essential character of the finished article.
  - Whether there is a change in tariff classification.
- Test can be confusing and inconsistently applied.

Biden EO and New Proposed Buy American Rules

- Biden Executive Order on Made in America
  - Established a Made in America Office within The Office of Management and Budget (OMB).
  - Required the Federal Acquisition Regulation Council (FAR Council) to examine the current Buy American regulations and propose rules to strengthen BAA requirements.
- FAR Council issued proposed rules on July 30, 2021 -- Final or Interim Final to be released shortly.
  - Increasing the domestic content threshold in BAA acquisitions (immediate 55 percent to 60 percent and to 65 percent in two years and then to 75 percent in five years).
  - Adopting enhanced price preferences for critical products or items that include critical components.
  - Requiring contractors to report the domestic content of critical items delivered under federal contracts.
- FAR Council also asked for information relating to potential future changes driven by Biden EO:
  - IT exception to BAA
  - COTS waiver
  - Trade Agreement Act Renegotiation.

Potential Future Buy American Technology

- Department of Commerce and Department of Homeland Security Buy American recommendations
  - Federal Acquisition Regulatory Council review its procurement policies for ICT products, services and components.

"Additional consideration should be given to enhanced Buy American Act provisions that incentivize the production of ICT products and services with significant U.S. value add, including design contribution, and with tolerances for assembly in allied or partner nations"

- DOC and DHS did not elaborate on how that would be done.

Export Controls

Export Controls – Overview

Export control laws govern the export, re-export and transfer of goods, software, technology and services.

Two primary U.S. regimes:

- **Export Administration Regulations (EAR)**
  - Administered by the Bureau of Industry and Security (BIS) at the U.S. Department of Commerce.
  - Governs "dual-use" and less sensitive military items.
- **International Traffic in Arms Regulations (ITAR)**
  - Administered by the Directorate of Defense Trade Controls (DDTC) at the U.S. Department of State.
  - Governs defense articles and services.
- **Exports** include not only physical shipments of products from the United States but also electronic transmissions of information, oral discussions and providing access to technical data on networks, among other types of transfers.

EAR – Key Concepts

- **Items "subject to the EAR"** include the following:
  - Items in the United States.
  - U.S.-origin items wherever located.
  - Foreign made items incorporating more than a de minimis level of controlled content.
  - Certain foreign-made items that are the direct products of specified software and technology.
  - Certain foreign-made items that are the direct products of certain plants or major components thereof.
- The EAR impose **licensing requirements** based on the following:
  - Classification of the item within the Commerce Control List (CCL).
  - Country of Destination (includes "deemed exports" or transfers to nationals of a certain country wherever located).
  - End-Use.
  - End-user.

Commerce Control List Categories

0	Nuclear Materials, Facilities And Equipment (and Miscellaneous Items)
1	Materials, Chemicals, Microorganisms and Toxins
2	Materials Processing
3	Electronics
4	Computers
5	Part 1 -- Telecommunications and Part 2 -- Information Security
6	Sensors and Lasers
7	Navigation and Avionics
8	Marine
9	Aerospace and Propulsion

Entity List Designations

Entity List (15 C.F.R. 744.16)

- Identifies persons reasonably believed to be involved, or to pose a significant risk of being or becoming involved, in activities contrary to U.S. national security or foreign policy interests.
- The export, reexport and transfer of **items subject to the EAR** generally require a license to such entities. Except in certain limited cases, BIS has a policy of denial with respect to such license applications.

Commerce has designated a variety of Chinese companies on the Entity List. The most high profile designation has been of **Huawei** and its affiliates.

- BIS expanded the scope of items subject to the EAR with respect to Huawei to capture additional foreign-produced items by **expanding the foreign direct product rule**.
- For most other Chinese companies on the Entity List, these expanded rules do not apply.

EAR - MEU Rules

The Military end use / user rules (15 CFR 744.21 and 744.22).

- Imposes license requirements on the export, re-export, or transfer of certain items subject to the EAR (see Part 744 Supp 2) if exporter has **"knowledge"** that the item is destined for a "**military end-use" or "military end-user"** in China, Russia and Venezuela. Note: new expansive rules apply to Russia to capture all items subject to the EAR.
- While there is an explicit MEU list in the EAR (Part 744 Supp. 7) that identifies specific Chinese entities, Commerce has made clear that it expects parties to **conduct diligence** and confirm the recipient is not a "military end-user," which Commerce interprets very broadly, and no "military end-use."
- In addition, if an exporter has "knowledge" that the items are destined for a **"military-intelligence end use"** or a **"military-intelligence end user,"** in China, Russia, Venezuela, a license is required.

Emerging and Foundational Technology

Stemming from the **Export Control Reform Act of 2018 (ECRA),** Commerce has a mandate to identify and control **"emerging and foundational technology"** that warrants control. This process has not resulted in any sweeping controls but has been a topic of focus for potential regulation, particularly with respect to China.

Examples of technologies currently subject to limited controls that could be considered "emerging" and subject to new, broader controls include the following:

- Biotechnology
- Artificial intelligence and machine learning
- Position, navigation, and timing (PNT) technology
- Microprocessor technology
- Advanced computing technology
- Data analytics technology
- Quantum information and sensing technology
- Logistics technology
- Additive manufacturing
- Robotics
- Brain-computer interfaces
- Hypersonics
- Advanced materials
- Advanced surveillance technologies.

Sanctions

Akin Gump
STRAUSS HAUER & FELD LLP

U.S. Sanctions – How Do They Work?

Over 30 sanctions programs administered by the U.S. Department of the Treasury Office of Foreign Assets Control ("OFAC")

Sanctions broadly prohibit certain dealings involving:

Countries/Territories	Individuals or Entities	Conduct
• Iran • Syria • North Korea • Cuba • Regions of Crimea, Luhansk, and Donetsk • Venezuela (more limited) • Russia (more limited).	• Specially Designated Nationals (SDNs) • Entities subject to sectoral sanctions (SSIs) • Foreign Sanctions Evaders (FSEs) • **Chinese Military-Industrial Complex Companies (CMICs).**	• Material support for SDNs • Weapons of mass destruction (WMD) proliferation • Key Sectors of Russian Economy • International Terrorism • Crimea • Human rights abuses • Other (*very long list*).

U.S. Sanctions – How Do They Apply?

Primary Sanctions

- Requires U.S. jurisdiction, but jurisdiction can be *territorial* or *extraterritorial* (e.g., captures conduct outside the U.S. with some U.S. nexus).
- Causing or facilitating a violation or conspiring to violate.
- **Typical Consequence: Fine (Max ~$300K/violation).**

Secondary Sanctions

- Does not require U.S. jurisdiction, covers specific conduct contrary to U.S. foreign policy or national security interest, regardless of U.S. nexus.
- **Typical Consequence: SDN List Designation.**

Sanctions on Chinese Military Companies

Background

- On June 3, 2021, President Biden issued EO 14032, which affirms and redefines the Trump administration policy to target publicly traded securities of certain Chinese military companies-referred to now as "Chinese Military-Industrial Complex Companies ("CMICs").
- U.S. persons are prohibited from engaging in the purchase or sale of:
  - *Publicly traded securities of CMICs.*
  - *Securities that are derivative of publicly traded securities of CMICs.*
  - *Securities that are "designed to provide investment exposure" to CMIC securities.*

Key Takeaways

- **CMICs.** The administration replaced the previous CCMC list with a new list identifying 59 companies as CMICs (note that some CCMCs are not designated as CMICs).
- **Divestment Exemption.** The EO includes a one-year exemption allowing divestment from covered securities (calculated from the date the CMIC was publicly identified).
- **Amended FAQs.** OFAC issued numerous FAQs which clarify the scope of the EO's prohibitions, as well as the new "Non-SDN CMIC List."

CFIUS

Committee on Foreign Investment in the United States

Akin Gump
STRAUSS HAUER & FELD LLP

CFIUS – Overview

Who?

- The **C**ommittee on **F**oreign **I**nvestment in the **U**nited **S**tates

- Consists of:
  - Nine Executive Branch departments, headed by **Treasury.**
  - Five observing members.
  - Others can be added for specific reviews (e.g., Dept. of Transportation).

What?

- Conducts **national security reviews** of certain transactions:
  - Foreign **control** of a "U.S. business".
  - Certain **non-controlling investments** by foreign persons in **Technology, Infrastructure, Data (TID) U.S. businesses.**
  - Certain **covered real estate** transactions by foreign persons.

How?

- CFIUS has **authority** to:
  - Direct a filing / initiate a review.
  - Impose mitigation measures to address national security concerns.
  - Suspend transactions.
  - Recommend the President block pending transactions and order divestiture in completed transactions.

CFIUS – Key Trends

- **Continued heavy scrutiny of Chinese investments and transactions that have a China nexus**
- **Semiconductors**
- **Emerging Tech**
- **Sensitive Personal Data**
- **Compliance with Mandatory Reporting**
- **Non-notified Transactions.**

ICTS

Information & Communications Technology and Services

Akin Gump
STRAUSS HAUER & FELD LLP

ICTS Overview

- May 2019: President Trump issued EO 13873 “Securing the Information and Communications Technology and Services Supply Chain” (“ICTS EO”).
  - Declared a national emergency with respect to the ability of “foreign adversaries” to create and exploit vulnerabilities in information and communications technology and services in order to commit “malicious cyber-enabled actions.”
  - Allowed the Secretary of Commerce to prohibit transactions with foreign adversaries when the Secretary determines that such a transaction would threaten national security.
- August 2020-January 2021 – Trump issues EOs under this authority targeting specific Chinese apps.
- January 2021: Commerce published a proposed interim final rule implementing ICTS regulations that the Biden Administration allowed to take effect in March 2021.
  - Identifies potentially covered transactions as those involving “foreign adversaries” that pose an undue or unacceptable risk to U.S. national security.
  - Excludes certain transactions from the rule (i.e., transactions actively or previously reviewed by CFIUS).
  - Previews that a licensing/pre-clearance mechanism could be established.

Background on ICTS Rule – Subsequent EO

Biden Administration's EO 14034 Revokes Trump Administration's "App Ban" EOs

- Between August 2020 and January 2021: The Trump Administration issued three "App Ban" EOs, citing the same national emergency as the ICTS EO to justify banning TikTok, WeChat, and other Chinese apps from operating in the United States.
- Users of these apps sued and courts issued preliminary injunctions to prevent the implementation of the TikTok and WeChat App Ban EOs.
- June 2021: The Biden Administration issued EO 14034 "Protecting Americans' Sensitive Data from Foreign Adversaries," which revoked the Trump Administration's App Ban EOs. However, the EO affirmed that a threat exists with respect to "connected software applications" and ordered an "evidence-based review" of the issue.

WeChat

TikTok

Current Regulatory Framework

Transaction is potentially within the scope of the ICTS regulations (15 CFR Part 7) when:

1. Person or property subject to U.S. jurisdiction.
2. Property in which any foreign country or foreign national has an interest (including through an interest in a contract for the provision of the technology/service).
3. Transaction initiated, pending, or completed on or after January 19, 2021.
4. Involves one of the six enumerated ICTS categories: critical infrastructure; networking; hosting/storage of sensitive personal data; widely sold surveillance, monitoring, networking devices; widely used internet communications applications; emerging technology.

Commerce only has authority to take action when an ICTS Transaction involves "ICTS designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary." "Foreign Adversary" is currently defined as China (including Hong Kong), Cuba, Iran, North Korea, Russia and the Maduro regime.

"Undue or Unacceptable Risk" as defined by IFR:

- An undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation or maintenance of ICTS **in the United States**.
- An undue risk of catastrophic effects on the security or resiliency of the **U.S. critical infrastructure or digital economy**.
- Or, an unacceptable risk to the national security of the United States or the security and safety of United States persons.

If the above are met, Commerce may mitigate, prohibit, and/or unwind the transaction

Outbound Investment Screening?

The National Critical Capabilities Defense Act

- Would create a new **reverse CFIUS**-like interagency committee to review and potentially **block outbound investments** by U.S. businesses to **shift or relocate** any "**design, development, production, manufacture, fabrication, supply, servicing, testing, management, operation, investment, ownership** or any other essential elements involving "**national critical capabilities**" to a "**country of concern**" (e.g., China or Russia).

Key Provisions

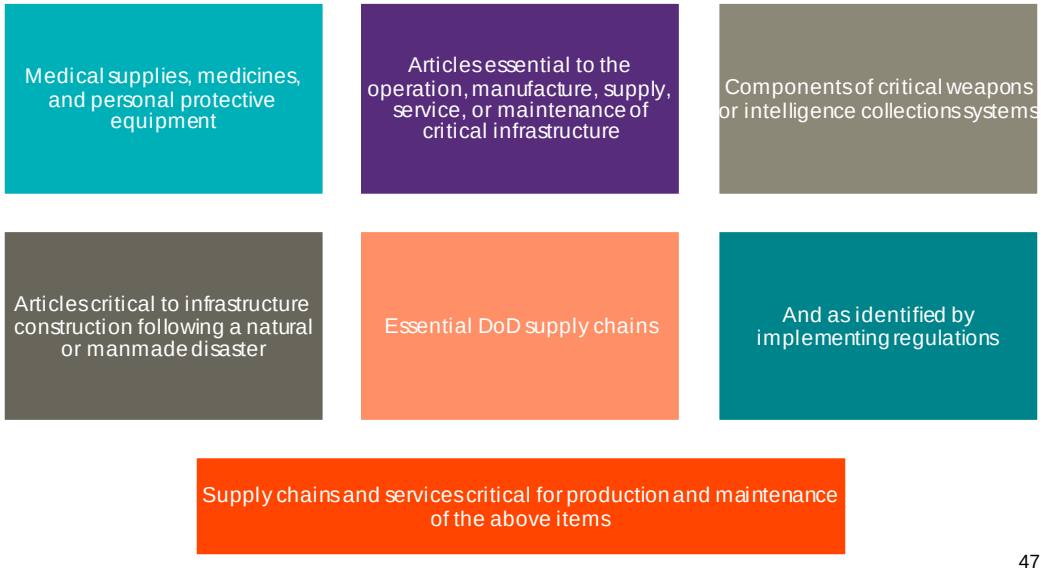
- Chaired by **USTR**, in consultation with Commerce and Defense.
- Following a 60-day review, any transaction identified by the committee as presenting an "**unacceptable risk**" to a **national critical capability** would be subject to **potential block**.
- All covered transactions would be subject to **mandatory filing**.
- **No monetary threshold**.
- Sponsors consider it apply to **off-shoring of existing manufacturing** as well as **greenfield capital expenditures**.

Status

- Originally introduced by Senators **Casey** (D-PA) and **Cornyn** (R-TX).
- Passed the House as part of the **America COMPETES** Act.
- **TBD** whether it makes it to the final conference version.

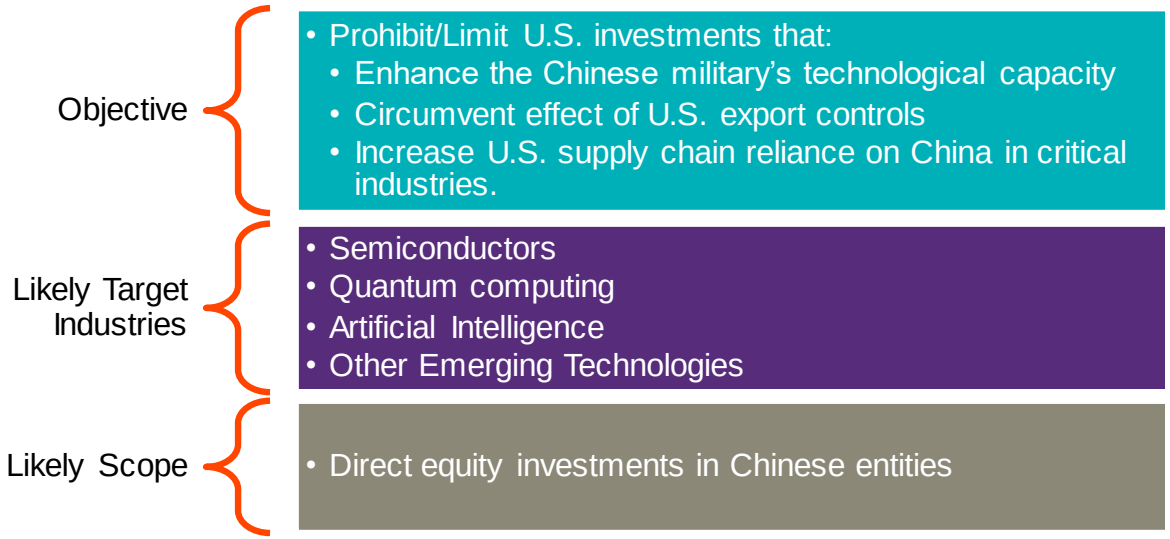
National Critical Capabilities

- "**Systems and assets** … so vital to the United States that the **inability to develop** such systems and assets or the **incapacity or destruction** of such systems or assets would have a **debilitating impact on national security or crisis preparedness**," such as:



Biden Administration Considers Executive Action

- Use of Presidential emergency economic authorities to implement outbound screening mechanism by **executive order** under consideration at the NSC.
  - Executive order to enact an outbound screening process relying on the President's authority under the International Emergency Economic Powers Act (**IEEPA**).
  - Result is likely to **more narrowly targeted** in scope than legislative efforts.



Alternatives to Outbound Screening?

Expand CMIC Sanctions beyond public securities to include venture capital funding or debt transactions?

Presenters

Christian C. Davis
Partner
Akin Gump Strauss Hauer & Feld LLP
Washington, D.C.
T: 202.887.4529
chdavis@akingump.com

Scott M. Heimberg
Partner
Akin Gump Strauss Hauer & Feld LLP
Washington, D.C.
T: 202.887.4085
sheimberg@akingump.com