

June 4, 2024

Gibson Dunn & Crutcher, LLP

Export Enforcement Trends 2024



Christopher T. Timura, Partner

David P. Burns, Partner

Melissa L. Farrar, Partner

Moderated by Samantha Sewall, Of Counsel

GIBSON DUNN

MCLE Certificate Information

MCLE Certificate Information

- Approved for 1.0 hour General PP credit.
- CLE credit form must be submitted by **Tuesday, June 11th**
- Form Link: https://gibsondunn.qualtrics.com/jfe/form/SV_9mYUExeFNWyajfE
 - Most participants should anticipate receiving their certificate of attendance in four to eight weeks following the webcast.
- **Please direct all questions regarding MCLE to CLE@gibsondunn.com.**

In the wake of Russia's further invasion of Ukraine and other challenges...

The Russian invasion of Ukraine “sparked a global response from governments and companies alike, and it elevated the importance of sanctions and export control enforcement.

What was once a technical area of concern for select businesses should now be at the top of every company's risk compliance chart.”

- Deputy Attorney General Lisa Monaco, March 2, 2023

...export controls have taken center stage.

“Our core mission – of preventing sensitive U.S. technologies and goods from being used for malign purposes by those who would do us harm – has perhaps never been a more important national security imperative than right now.”

- Assistant Secretary for Export Enforcement
Matthew S. Axelrod, April 25, 2024

Agenda

-
- 01** Introduction: The Rising Significance of Export Controls in U.S. National Security and Foreign Policy

 - 02** Evolution of Corporate Enforcement Policies – U.S. Department of Commerce and U.S. Department of Justice

 - 03** Increasing Coordination and Resources for Export Enforcement, Both At Home and Abroad

 - 04** Notable Recent Enforcement Actions by DOJ and BIS



 - 05** Conducting a Successful Export Controls Investigation and Weighing the Decision to Self-Disclose

Evolution of BIS enforcement policy since 2022


New statement of BIS enforcement policy focuses on:

- Higher civil penalties for serious or “egregious” violations
- Admission of wrongdoing
- Fast-tracking of minor or technical violations
- Increased use of non-monetary penalties, i.e. training, compliance program enhancements, and suspended denial orders

Violations of the EAR are defined at 15 C.F.R. 764.2 and under the Export Control Reform Act of 2018, 50 U.S.C. 4801-4852, 4819.

	UNITED STATES DEPARTMENT OF COMMERCE Assistant Secretary for Export Enforcement Washington, D.C. 20230
June 30, 2022	
MEMORANDUM FOR ALL EXPORT ENFORCEMENT EMPLOYEES	
FROM:	MATTHEW S. AXELROD  ASSISTANT SECRETARY FOR EXPORT ENFORCEMENT
SUBJECT:	FURTHER STRENGTHENING OUR ADMINISTRATIVE ENFORCEMENT PROGRAM
<p>As you all know, this year marks the 40th anniversary of the Office of Export Enforcement. For forty years, special agents from OEE have been on the frontlines, alongside our intelligence analysts and enforcement compliance specialists, ensuring that our most sensitive items stay out of the most dangerous hands. During those forty years, the national security threat picture has evolved</p>	

Evolution of DOJ self-disclosure policy since 2020



Department of Justice

Updated March 7, 2024
www.justice.gov

NSD
(202) 514-2007

NSD ENFORCEMENT POLICY FOR BUSINESS ORGANIZATIONS¹

Introduction

The mission of the National Security Division (NSD) of the Department of Justice is to carry out the Department's highest priority: to protect and defend the United States against the full range of national security threats, consistent with the rule of law. Business organizations and their employees are at the forefront of NSD's efforts to protect the national security of the United States by preventing the unlawful export of sensitive commodities, technologies, and services, as well as unlawful transactions with sanctioned countries and designated individuals and entities. Enforcing our export control and sanctions laws, and holding accountable those who violate them, is a top priority for NSD.

The National Security Division (“NSD”) handles criminal enforcement of U.S. export control and sanctions laws, among other matters related to national security.

Under *Bryan v. United States* (1998), an act is willful if done with the knowledge that it is illegal. The government, however, is not required to show the defendant was aware of the specific law, rule, or regulation that its conduct may have violated.

Criminal violations of the EAR carry penalties up to \$1 million USD fine, imprisonment up to 20 years, and criminal forfeiture. See 50 U.S.C. § 4819.

DOJ National Security Division expectations

Prompt disclosure directly to NSD of all potentially criminal violations of the Arms Export Control Act (22 U.S.C. § 2778), the Export Control Reform Act (50 U.S.C. § 4819), or the International Emergency Economic Powers Act (50 U.S.C. § 1705), *as well as potential violations of other criminal statutes that affect national security* when they arise out of or relate to enforcement of export control and sanctions laws.

When a company:

- (1) voluntarily self-discloses to NSD potentially criminal violations arising out of or relating to the enforcement of export control or sanctions laws,
- (2) fully cooperates, and
- (3) timely and appropriately remediates,

absent aggravating factors, NSD generally **will not seek a guilty plea, and there is a presumption that the company will receive a non-prosecution agreement and will not pay a fine.**



DOJ factors in enforcement response

Fully qualified self-disclosure

Made directly to NSD.

At the earliest possible time.

Disclose all non-privileged facts, including evidence of individuals involved in or responsible for the misconduct, whether inside or outside the organization.

Proactive and continuing cooperation

Proactive and continuing disclosure of all relevant non-privileged facts.

Identifying opportunities to obtain relevant evidence not in the company's possession.

Overcoming hurdles to foreign document production.

Making individuals available for interviews.

Remediation

Conduct a root cause analysis.

Implement an effective compliance and ethics program that is sufficiently independent, authorized, and resourced.

Compensation clawback from employees engaged in misconduct or managers who failed to provide oversight.

Retention of business records (including messaging apps and personal devices).

Aggravating factors

Pervasive and egregious conduct, including repeat violations.

Concealment or involvement by upper management.

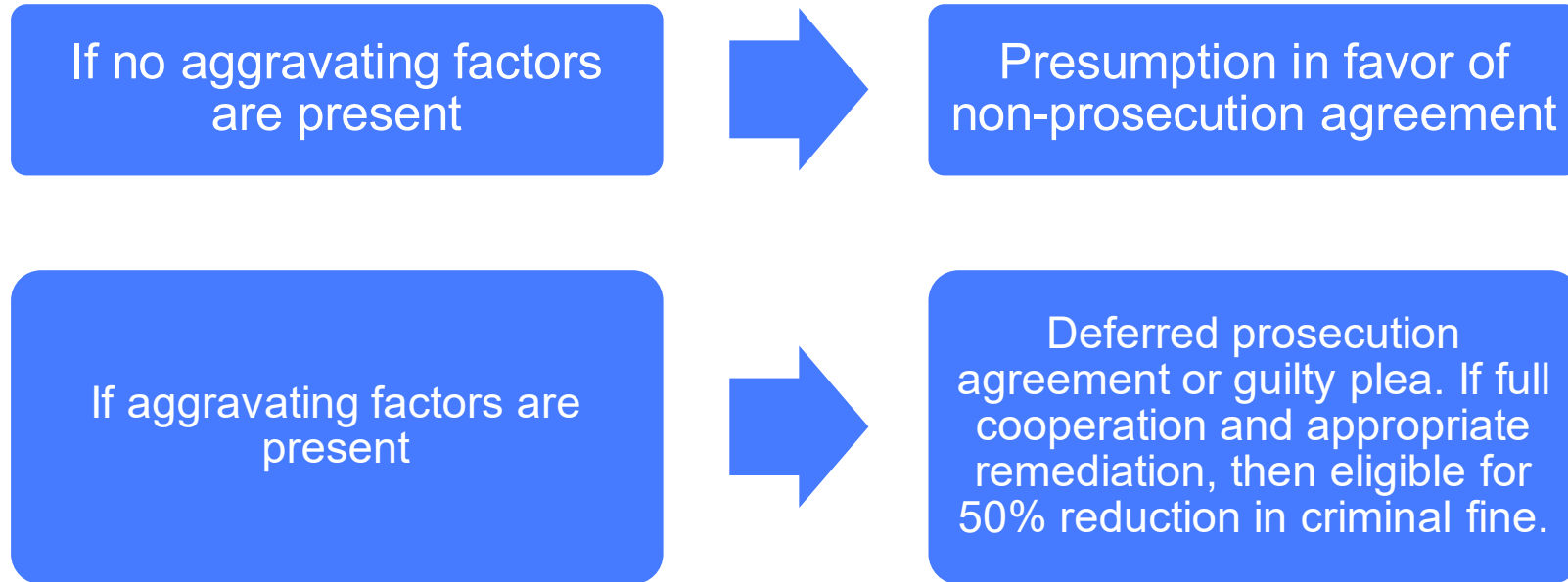
Significant profit from misconduct.

Involvement with Foreign Terrorist Organizations or Specially Designated Global Terrorists.

Exports of items controlled for non-proliferation or missile technology reasons.

Exports of WMD components or military items to countries of concern.

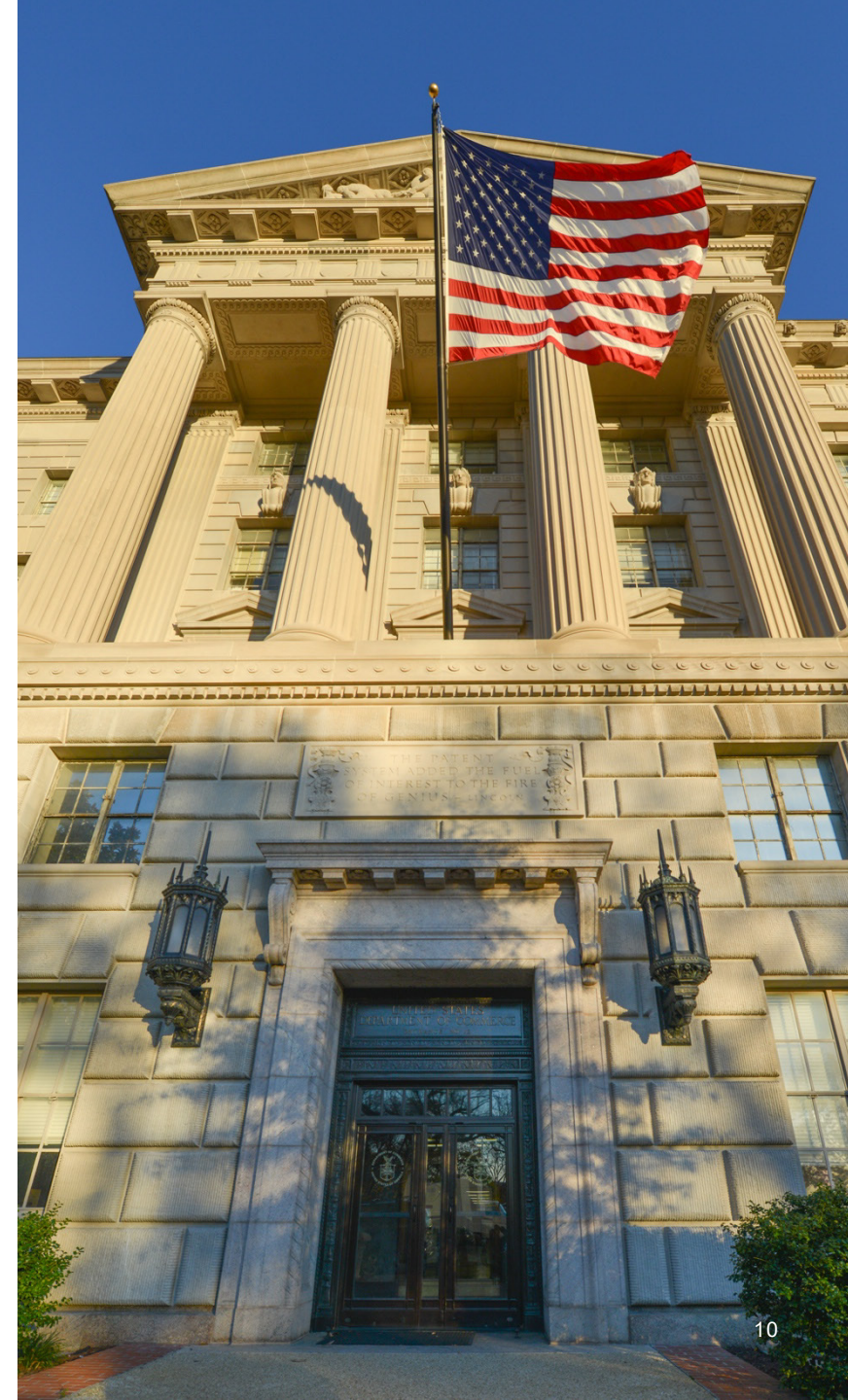
Benefits of self-disclosure



M&A Policy - If the acquiror meets the factors in the VSD policy, it can also earn the benefits set forth in the policy when it self-discloses misconduct of an acquired company within 180 days of acquisition.

Coordination among DOJ, Commerce, FBI, DHS, and others

- Announced in February 2023, the **Disruptive Technology Strike Force** including DOJ, BIS, the Federal Bureau of Investigation, the Department of Homeland Security, and regional U.S. Attorney's Offices to target criminal violations of export control laws.
- Enforcement authorities are focused on **third-party intermediaries** (agents, brokers, resellers) and the **use of transshipment points** in areas of higher risk
- Examples cited by BIS: Armenia, Brazil, China, Georgia, India, Israel, Kazakhstan, Kyrgyzstan, Mexico, Nicaragua, Serbia, Singapore, South Africa, Taiwan, Tajikistan, Turkey, United Arab Emirates, and Uzbekistan.
- In March 2023, Deputy Attorney General Lisa Monaco announced that **DOJ would be hiring 25 new prosecutors** devoted to bringing cases under export control and sanctions laws. The DOJ also appointed its first-ever **Chief Counsel for Corporate Enforcement within NSD**.



Coordination among BIS and the Financial Crimes Enforcement Network



In June 2022, May 2023, and November 2023, BIS and the Financial Crimes Enforcement Network (“FinCEN”) of the Treasury Department issued first-of-their-kind joint notices to financial institutions requesting that banks, credit card operators, and foreign exchange dealers report suspicious transactions related to **potential violations of export controls on Russia or the EAR generally** to FinCEN and identify such reports with a unique export-related SAR code.

FIs are asked to identify **high priority HTS codes** in trade documentation, new importers established after February 2022, increased sales to diversion points, and other **red flags** related to export transactions.

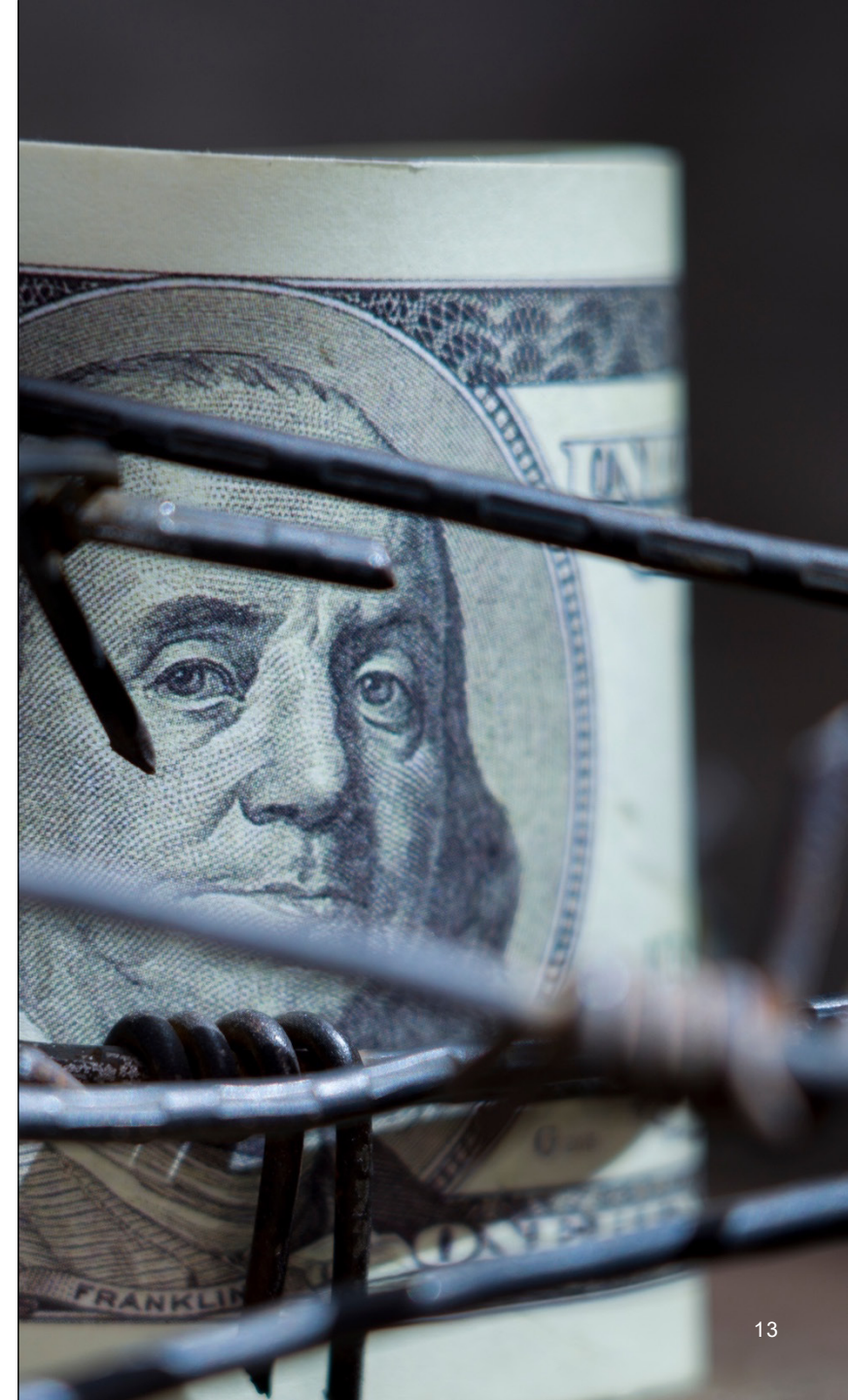


International cooperation

- Export Enforcement Five (“E5”): Australia, Canada, New Zealand, the United Kingdom, and the United States announced on June 28, 2023, their agreement to coordinate and exchange information related to enforcement of export controls on Russia and Belarus. [Press Release](#).
- G7 Enforcement Coordination Mechanism: United States, United Kingdom, Germany, France, Italy, Canada, Japan, and the EU have agreed to coordinate efforts to bolster enforcement of multilateral sanctions and export controls aimed at denying Russia the inputs its needs to equip its military and fund its illegal war. April 27, 2023 [Readout](#).
 - Global Export Control Coalition (“GECC”), a group of now 39 nations that have agreed to implement similar controls on Russia and Belarus.
- Disruptive Technology Protection Network: Japan and Republic of Korea have entered into agreements with the United States to coordinate on export control enforcement investigations. Launched April 25, 2024. [Press Release](#).
- European Anti-Fraud Office (“OLAF”): BIS and OLAF entered into an administrative cooperation agreement, focusing particularly on the exchange of strategic information, risk analysis, and assistance in investigations. March 20, 2023, [Press Release](#).

Case Study: MilliporeSigma Declination

- MilliporeSigma, a North American affiliate of Germany-based conglomerate Merck, offered discount buying programs for institutional clients, including universities.
- Between 2016 and 2023, two U.S. citizens – one an employee of the company – conspired to order chemical products at a discount **by fraudulently representing that the purchaser was a Florida university**. Conspirators later **diverted** the products to China.
- Conspirators provided **false export information** in the Automated Export System, maintained by U.S. Customs and Border Protection, that misstated the value and nature of the products.
- Shipments included List 1 chemicals, analytical samples of controlled substances (e.g. cocaine, morphine, codeine, fentanyl), and purified noncontagious proteins of contagious diseases (e.g. cholera toxin).
- MilliporeSigma self-disclosed to NSD **one-week** after retaining external counsel to conduct an internal investigation.
- Conspirators entered guilty pleas, while MilliporeSigma received a **declination and no monetary penalty, disgorgement, forfeiture, or restitution was required**.



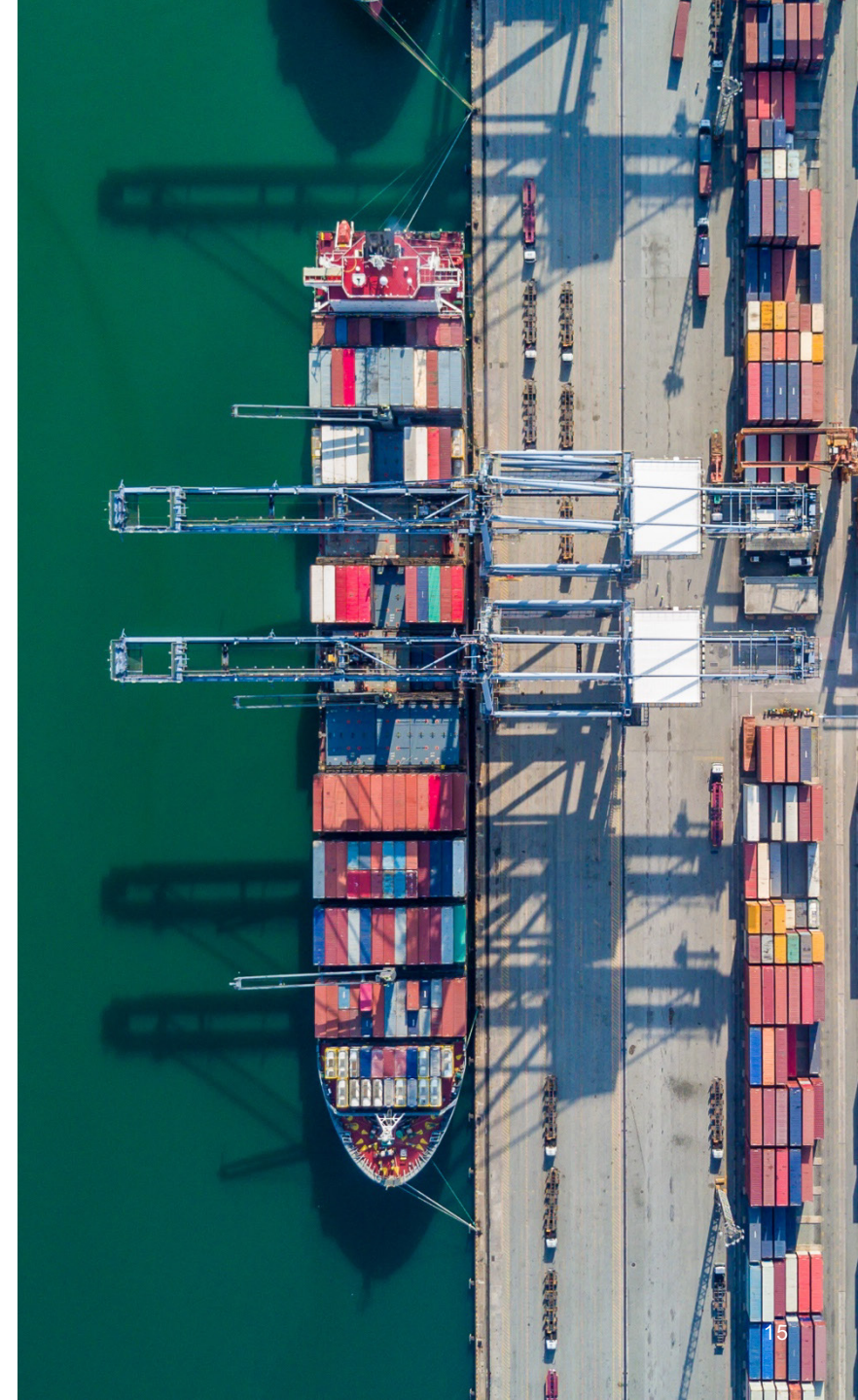
Case Study: SAP

- **First-ever resolution** pursuant to the NSD's Export Control and Sanctions Enforcement Policy.
- SAP, a German-headquartered global software company, **self-disclosed** to DOJ, Commerce, and Treasury the illegal export of its software to Iran.
- As a result of its voluntary disclosure to DOJ, extensive cooperation and strong remediation, costing more than \$27 million, SAP received a **Non-Prosecution Agreement (“NPA”)**.
- Under the NPA, SAP would pay a criminal fine of \$8 million (as part of a global resolution) and disgorge \$5 million of profits from the illegal exports. [DOJ Press Release](#), April 29, 2021.



Case Study: Seagate Technology, LLC

- In April 2023, **BIS imposed a \$300 million civil penalty against Seagate Technology LLC of Fremont, CA and Seagate Singapore International Headquarters Pte. Ltd.** of Singapore to resolve alleged violations of U.S. export controls related to selling hard disk drives (“HDD”) to Huawei Technologies Co. Ltd. in violation of the Huawei-related foreign direct product rule.
- One month after the new **Huawei-related foreign direct product rule (“FDPR”)** went into effect in 2020, Seagate entered into a new preferred supplier agreement with Huawei. Over 7 million hard drives were shipped to Huawei, worth over \$1 billion. Two closest competitors publicly announced end of sales to Huawei.
- In addition to the fine of \$300 million, **BIS required a multi-year compliance audit, and a 5-year suspended denial order.** Penalty was approximately double the company’s profits from the misconduct.
- A **supplier warned** Seagate that the equipment it provided, if used to manufacture items outside of the U.S., the products could be subject to the Huawei FDPR.
- Under the new BIS enforcement policy, a tip to BIS can earn future mitigation credit.



Conducting an export control investigation: **overview**

Increased focus by NSD on export controls counsels swift, thorough, and formal investigation of potential criminal export control violations.

Key steps include:

- Establishing and protecting privilege
- Scoping the investigation
- Data preservation and collection
- Interview preparation and execution
- Written analysis
- Disclosure analysis and government engagement



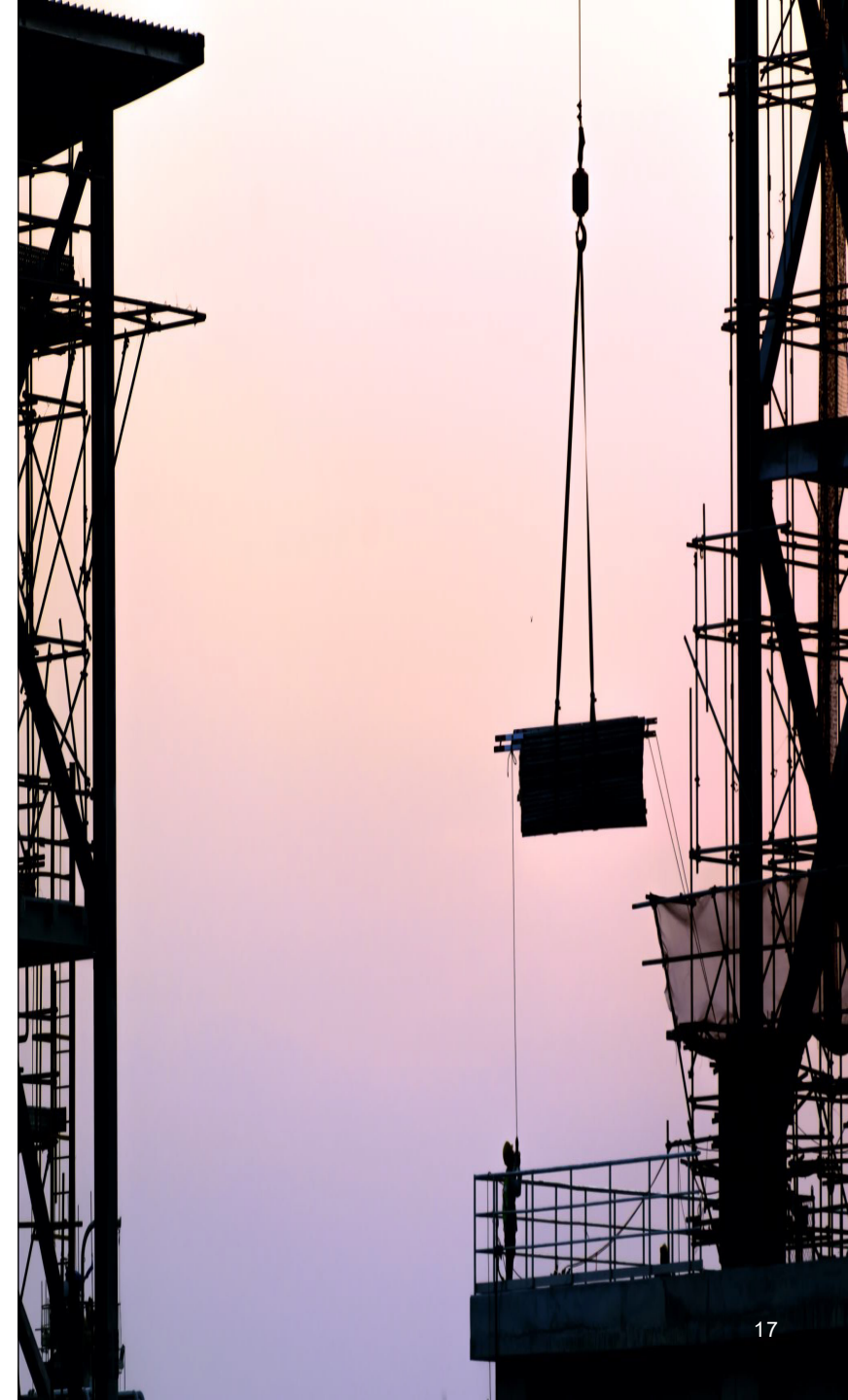
Conducting an export control investigation: **first steps**

Key initial questions:

- How did the issue or allegation arise?
- What is the alleged or apparent severity of the violation?
- Are there indications or allegations of willfulness or recklessness?
- Are there apparent aggravating factors?
- What is the likelihood of this allegation or issue becoming known externally?

Answers may help guide:

- Who conducts the investigation (internal or external counsel, attorneys or non-attorneys);
- Agencies to which disclosure is made;
- Timing and sequencing of any disclosure.



Conducting an export control investigation, continued

Protecting Privilege:

- Any export control allegation or violation with any level of criminal flavor should be investigated at the direction of (in-house or external) counsel.
- Do not expect privilege protection over any communications before counsel is actively engaged and involved.
- Limit sharing of investigative information to those within the Company who have a “need to know” of the content of the investigation. Expanding beyond this circle risks privilege waiver.
- Similarly, be very thoughtful about seeking information from outside the company (e.g., vendors, former employees), as content outside the scope of their engagement/employment may not be covered.
- Be intentional about using “attorney-client privilege” and “work product” branding on communications, as appropriate – and try not to over-use them.
- Give *Upjohn* warnings to interviewees and internal subject matter expert contributors to the investigation.



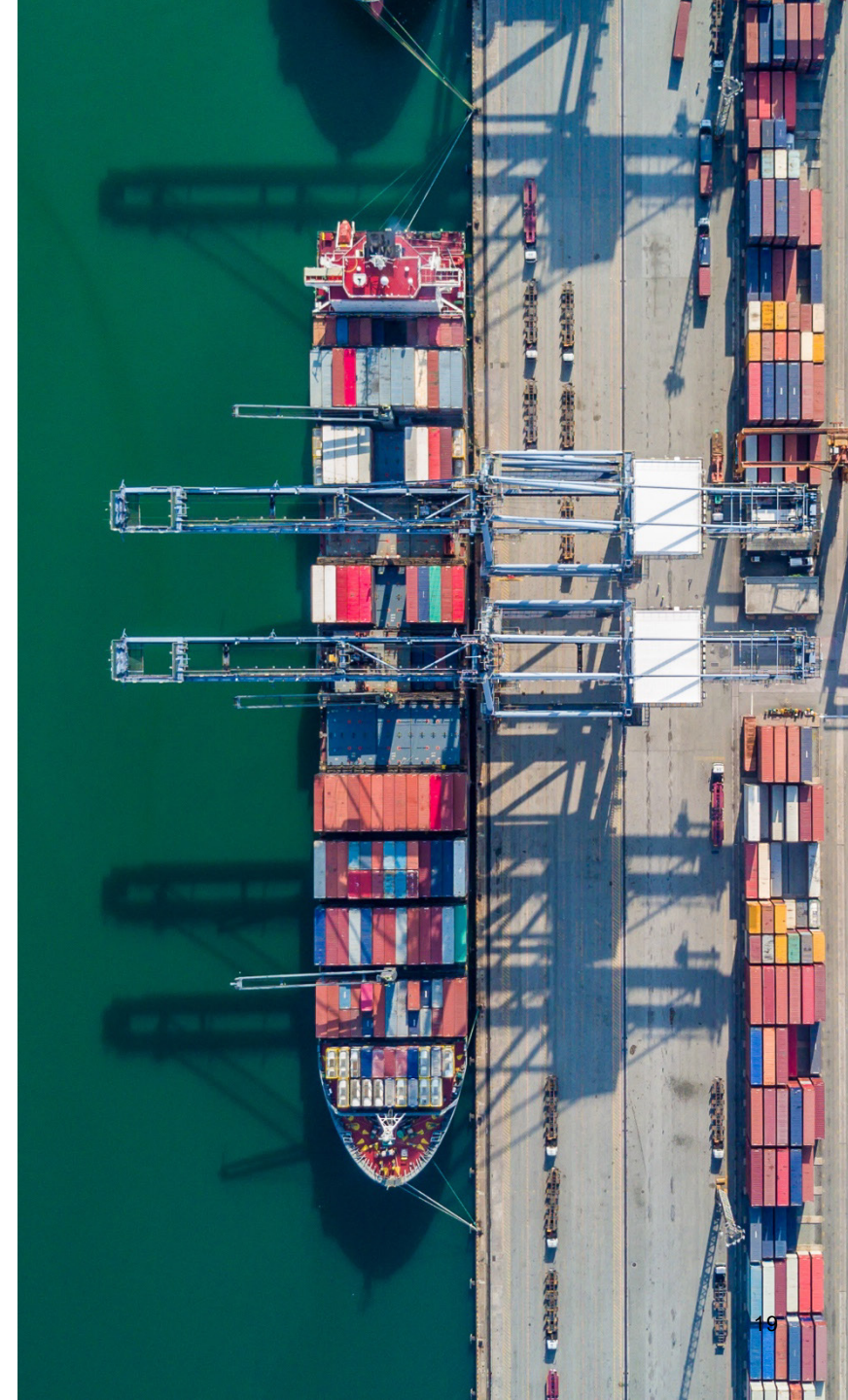
Conducting an export control investigation, continued

Scoping and Tailoring the Investigation:

- Engage with the individual who first raised the concern, under privilege, to obtain as much information as possible about the nature of the possible violation, the circumstances surrounding it, who was involved, and what documents or other relevant materials may exist.
- Conduct any limited diligence necessary using public or internal resources to evaluate the initial report.
- Follow the evidence, broadening or narrowing the investigative scope as appropriate given the nature of the report.
- Be careful to avoid tipping off any alleged wrongdoers prematurely.

Key questions at this stage:

- What questions need answering to evaluate the report?
- Who to interview?
- Whose emails/chats/mobile data and documents to collect?
- What other sources of information to tap?



Conducting an export control investigation, continued

Data Preservation and Collection:

- Ensure back-end preservation of documents and data before engaging with any possible wrongdoers, and to avoid data loss if any key witness or participant leaves the company.
- Consider the use of appropriately scoped legal holds.
- Consider the relative benefits and drawbacks of “quiet” collections vs employee-assisted targeted collections.
 - What collections require alerting the user?
 - What collections are not possible without employee participation?
- Consider limitations on potentially key data available for collection (ephemeral messages, etc.).
- Be mindful of international laws and regulations that could impact how information is collected (GDPR, state secrets, etc.)

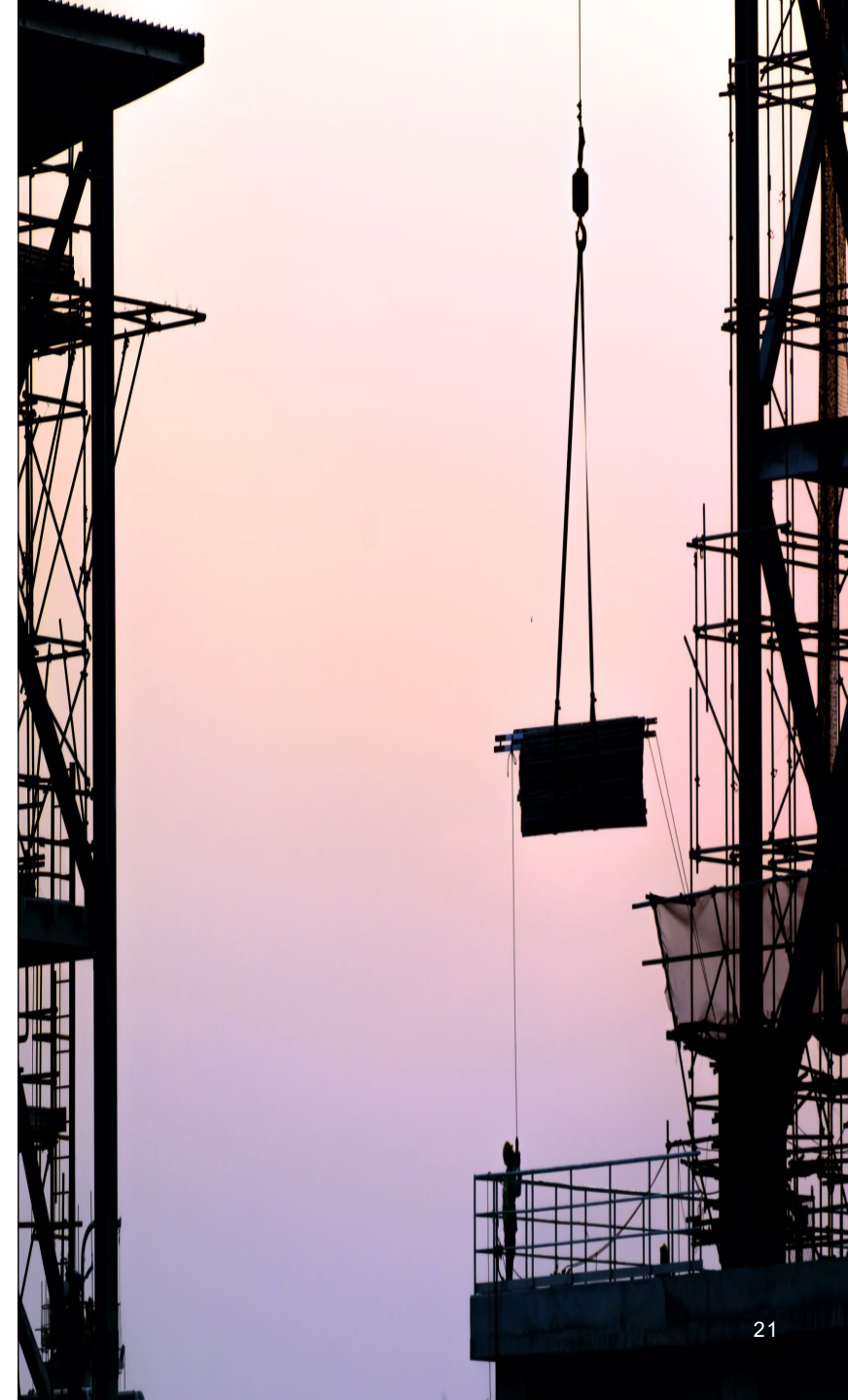


Conducting an export control investigation, continued

Interviews:

- Conduct interviews under privilege.
- Consider the order of interviews (traditional wisdom is witnesses first, subjects last).
- Consider timing (both in terms of where interviews fall in the timeline against data collection/ingestion, and how much time to schedule with each interviewee).
- Organize documents you want to use and outline topics/questions.
- Consider who is present during the interview, and how those dynamics might impact a particular interviewee's responses.
- Consider the venue (in-person versus video) and the interviewee's environment.
- Memorialize interviews in a manner consistent with confidentiality, privilege, and local law.

After interviews, pause and ask: have all questions been answered? Are there new questions that merit further assessment?



Conducting an export control investigation, continued

Written analysis:

- If the final work product is a VSD submission, balance regulator expectations of complete and deferential disclosures, including admissions of wrongdoing, against the dangers of making admissions in the criminal context.
- Consider opportunities for oral versus written submissions.
- Consider joint versus separate briefings for multi-agency enforcement actions.
- Privilege (and privilege waiver) will be a thorny consideration where the company received advice of counsel (internal or external) to guide the course of action under scrutiny.

Disclosure assessment:

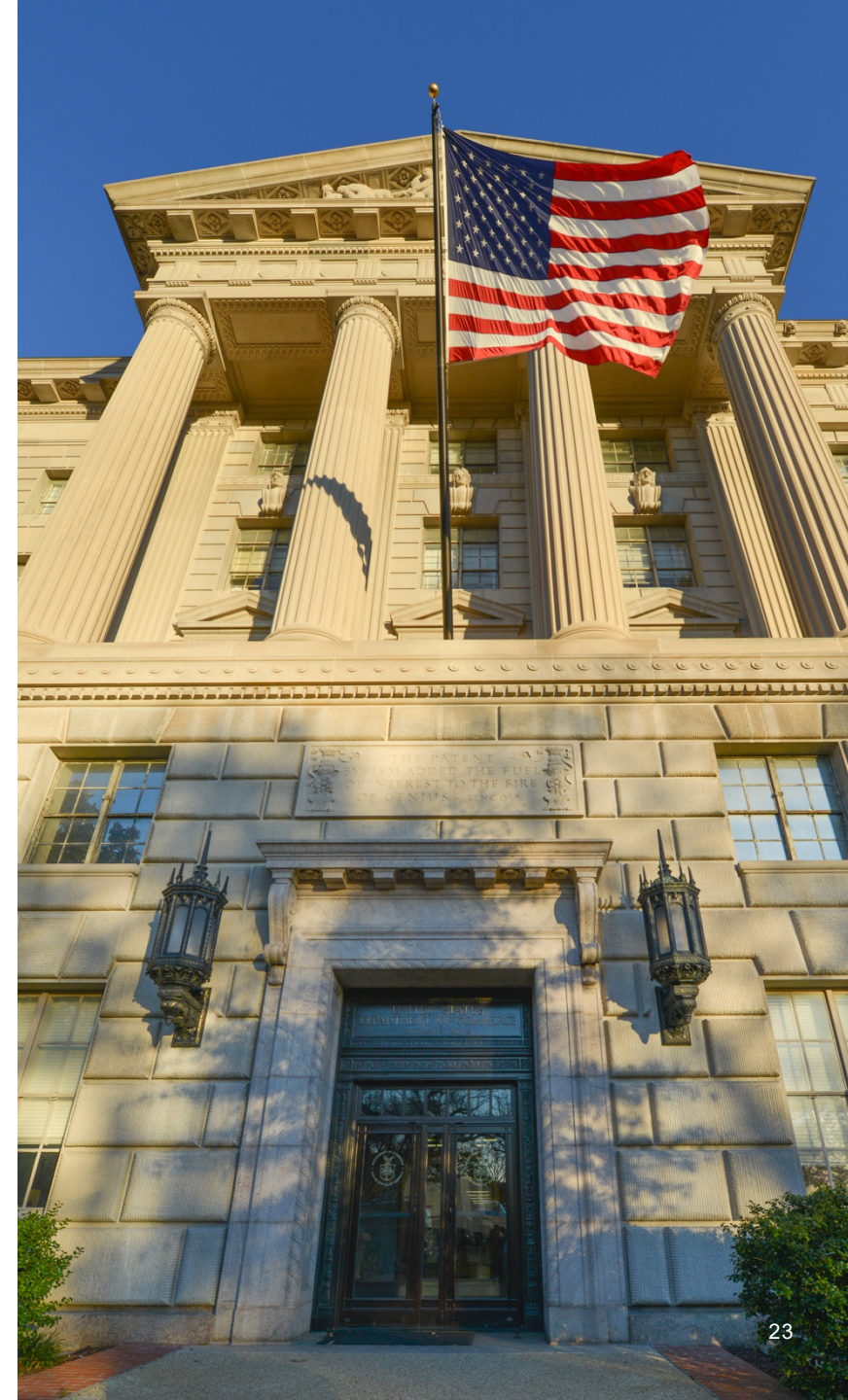
- In the export control context, a VSD decision likely will need to be made before the conclusion of the investigation, weighing the factors discussed earlier.
- If a decision not to self-disclose is made in early stages, this decision should be continuously reassessed.
- NSD policy effectively requires concurrent disclosures to NSD and other agencies.



Navigating the **new export enforcement environment**

Best practices:

- Check in with internal legal and compliance resources to confirm effectiveness of internal controls and export classification of products and technology.
- Ensure that employees know where to report potential violations.
- Confirm that employees know where to refer government inquiries.
- Be alert to all facts and circumstances that suggest potential willful violations of export control laws.
- Incorporate appropriate controls to ensure preservation of privilege and document retention.
- Carefully consider all factors relevant to self-disclosure.



Attorney Bios

Christopher T. Timura

Partner / Washington, D.C.

Christopher T. Timura is a partner in the Washington D.C. office of Gibson, Dunn & Crutcher LLP and a member of the firm's International Trade and White Collar Defense and Investigations Practice Groups.

He helps clients solve regulatory, legal and political problems that arise at the intersection of national security, trade, and foreign policy, and to develop corporate social responsibility (CSR) and environmental, social, and governance (ESG) strategies, policies, and procedures. His clients span economic sectors and range from start-ups to Global 500 companies. Most recently, Christopher was ranked in the *Chambers Global 2024* guide for USA International Trade: Export Controls & Economic Sanctions.

Christopher counsels clients on compliance with U.S. export controls (ITAR and EAR), economic sanctions, and foreign investment reviews and represents them before the departments of State (DDTC), Treasury (OFAC and CFIUS), Commerce (BIS), Homeland Security, and Justice in voluntary and directed disclosures, civil and criminal enforcement actions and investment reviews. Working with in-house counsel, boards, and other business leads, he helps to identify and leverage existing business processes to integrate international trade compliance, and CSR-related data gathering, analysis, investigation, and reporting throughout client business operations. In M&A and other transactions, he conducts expedited diligence on international trade compliance and ESG issues and supports business and compliance teams as they work to spin off or integrate business operations in new organizations.

He also assists clients working with emerging and foundational technologies in the development of effective international trade compliance-, export control licensing-, and CSR-strategies to support global R&D, supply chain, and customer bases.

Christopher's full biography is available [here](#).



EDUCATION

University of Michigan
Ph.D.

University of Michigan
Juris Doctor

University College London
Master of Science

Denison University
Bachelor of Arts



David P. Burns

Partner / Washington, D.C.

1050 Connecticut Avenue, N.W., Washington, D.C. 20036-5306

+1 202.887.3786

dburns@gibsondunn.com

David P. Burns is a litigation partner in the Washington, D.C., office of Gibson, Dunn & Crutcher. He is the co-chair of the firm's National Security Practice Group, and a member of the White Collar and Investigations and Crisis Management practice groups. His practice focuses on white-collar criminal defense, internal investigations, national security, and regulatory enforcement matters. David represents corporations and executives in federal, state, and regulatory investigations involving securities and commodities fraud, sanctions and export controls, theft of trade secrets and economic espionage, the Foreign Agents Registration Act, accounting fraud, the Foreign Corrupt Practices Act, international and domestic cartel enforcement, health care fraud, government contracting fraud, and the False Claims Act.

Prior to re-joining the firm, David served in senior positions in both the Criminal Division and National Security Division of the U.S. Department of Justice. Most recently, he served as Acting Assistant Attorney General of the Criminal Division, where he led more than 600 federal prosecutors who conducted investigations and prosecutions involving securities fraud, health care fraud, Foreign Corrupt Practices Act violations, public corruption, cybercrime, intellectual property theft, money laundering, Bank Secrecy Act violations, child exploitation, international narcotics trafficking, human rights violations, organized and transnational crime, gang violence, and other crimes, as well as matters involving international affairs and sensitive law enforcement techniques. Prior to joining the Criminal Division, David served as the Principal Deputy Assistant Attorney General of the National Security Division from September 2018 to December 2020. In that role, he supervised the Division's investigations and prosecutions, including counterterrorism, counterintelligence, economic espionage, cyber hacking, FARA, disclosure of classified information, and sanctions and export controls matters. He also spent five years as an Assistant United States Attorney in the Southern District of New York, Criminal Division, from 2000 to 2005.

David graduated in 1995 from Columbia Law School, where he was a Harlan Fiske Stone Scholar and an Articles Editor of the *Columbia Business Law Review*. He received his Bachelor of Arts degree in economics from Boston College in 1991.

David's full biography is available [here](#).

EDUCATION

Columbia University
Juris Doctor

Boston College
Bachelor of Arts



EDUCATION

The George Washington University
Juris Doctor

Dartmouth College
Bachelor of Arts

Melissa L. Farrar

Partner / Washington, D.C.

Melissa Farrar is a partner in the Washington, D.C. office of Gibson, Dunn & Crutcher, where she practices primarily in the areas of white collar defense and investigations and corporate compliance. She also maintains a practice in government contracts compliance and litigation.

Melissa has experience representing and advising multinational corporations in internal and government investigations on a wide range of topics, including compliance with the U.S. Foreign Corrupt Practices Act and other anti-corruption laws, anti-money laundering, and tax. She has conducted fieldwork in Asia, Europe, Latin America, and the United States.

She has been recognized by the 2024 edition of *Best Lawyers: Ones to Watch® in America* for Criminal Defense: White-Collar. She was named by Expert Guides in its 2021 and 2022 *Rising Stars Guide*, which recognizes the brightest and most talented practitioners under 40 in the area of business law and related practices.

Melissa also counsels corporations on the effectiveness of their compliance programs and in connection with transactional due diligence, with a particular emphasis on compliance with anti-corruption laws.

Melissa received her law degree with high honors from the George Washington University Law School in 2013, where she was elected to the Order of the Coif. While in law school, she was a member of the George Washington Law Review. She received her Bachelor of Arts degree in 2004 from Dartmouth College.

Melissa is admitted to practice in the District of Columbia.

Melissa's full biography is available [here](#).

Samantha Sewall

Of Counsel / Washington, D.C.

Samantha Sewall is of counsel in the Washington, D.C. office of Gibson, Dunn & Crutcher and a member of the firm's International Trade Practice Group.

She advises clients on compliance with U.S. legal obligations at the intersection of global trade, foreign policy, and national security, focusing her practice on compliance with U.S. economic sanctions, export controls, national security reviews of foreign direct investment (CFIUS), and anti-boycott laws. Samantha has experience advising companies across a wide range of sectors including aerospace, banking and financial institutions, defense, energy, medical devices and pharmaceuticals, shipping, retail, telecommunications, and travel.

On a *pro bono* basis, Samantha has assisted clients with understanding U.S. trade controls and immigration issues, and she has worked with an international rule of law NGO to support law enforcement training efforts to combat transnational human trafficking and forced labor.

Prior to joining Gibson Dunn, she served as a Political-Economic Program Assistant supporting the U.S. Embassy in Côte d'Ivoire. During her time there she was responsible for programs and research related to private sector engagement and bilateral political and economic issues. Samantha was previously an associate with a large international law firm where she was a member of the international trade and investment practice group.

Samantha graduated *magna cum laude* from Georgetown University Law Center in 2012, where she was elected to the Order of the Coif and was a member of the Georgetown Law Journal. She is admitted to practice in the Commonwealth of Virginia, the District of Columbia, and the U.S. Court of International Trade.

Samantha's full biography is available [here](#).



EDUCATION

Georgetown University
Juris Doctor

Patrick Henry College
Bachelor of Arts

GIBSON DUNN