

# Sanctions and Export Controls

An aerial photograph of a large container ship sailing on the dark blue ocean. The ship's deck is densely packed with multi-colored shipping containers in shades of red, blue, yellow, and orange. The ship's superstructure and bridge are visible at the top right of the frame.

## Key Regulatory and Enforcement Trends

October 17, 2024

**GIBSON DUNN**

# MCLE CERTIFICATE INFORMATION

## MCLE Certificate Information

- Approved for 1.0 hour General PP credit.
- CLE credit form must be submitted by **Thursday, October 24<sup>th</sup>**
- Form Link: [https://gibsondunn.qualtrics.com/jfe/form/SV\\_7P9Jbl4aiLpuwm](https://gibsondunn.qualtrics.com/jfe/form/SV_7P9Jbl4aiLpuwm)
  - 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](mailto:CLE@gibsondunn.com).**

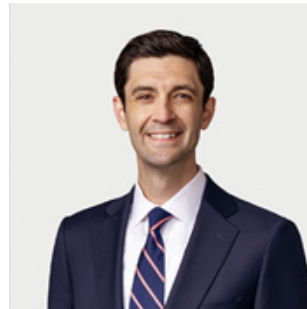
# Today's Presenters



**Adam M. Smith**

**Partner; Co-Chair,  
International Trade,  
Washington, D.C.**

asmith@gibsondunn.com



**Scott R. Toussaint**

**Senior Associate,  
Washington, D.C.**

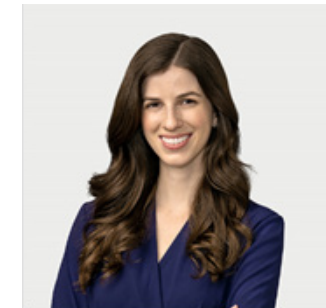
stoussaint@gibsondunn.com



**Christopher T. Timura**

**Partner,  
Washington, D.C.**

ctimura@gibsondunn.com



**Anna Searcey**

**Associate,  
Washington, D.C.**

asearcey@gibsondunn.com

# AGENDA

- 01** Key Concepts in U.S. Sanctions
- 02** Key Concepts in U.S. Export Controls
- 03** Regulatory Trends
- 04** Enforcement Trends
- 05** Weighing the Decision to Self-Disclose
- 06** Conducting Successful Investigations

# KEY CONCEPTS IN U.S. SANCTIONS

01

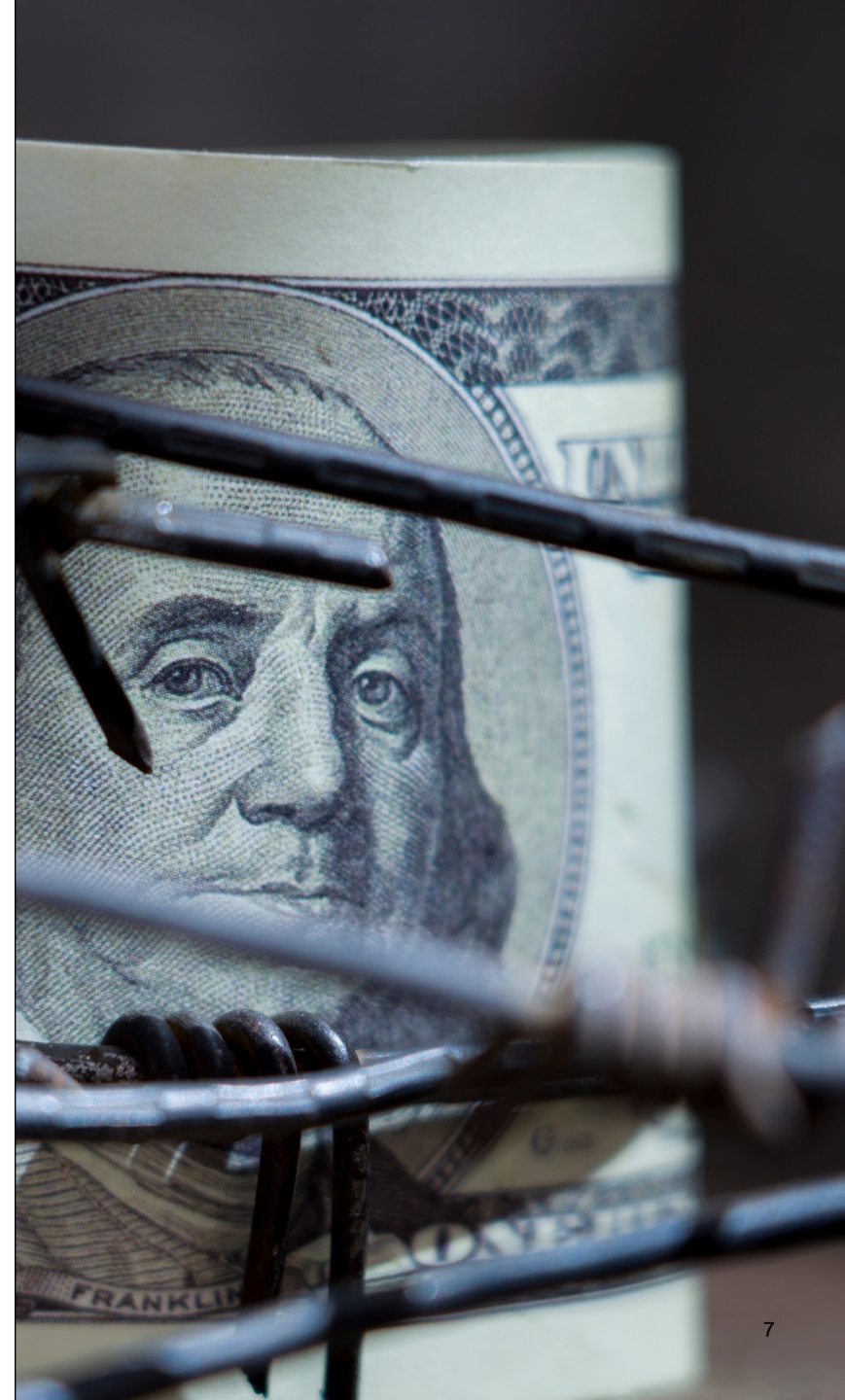
# Primary Agencies

- Office of Foreign Assets Control (OFAC) at Treasury
- Department of State
- Global & Non-U.S. Rules



# The Rules

- U.S. Statutes
  - IEEPA and TWEA
  - Others
- Executive Orders
- Regulations
- Directives
- Licenses and Exemptions
- Guidance



# Compliance Obligations: U.S. Persons

- **U.S. Persons**
  - U.S. persons include citizens and permanent residents of the United States, entities organized under U.S. state or federal law (including their foreign branches), and any person in the United States
  - Must comply with U.S. sanctions at all times and globally, or else face potential civil and criminal liability
- **Non-U.S. Persons**
  - Non-U.S. persons as a general matter do *not* fall under U.S. jurisdiction and their obligation to comply with U.S. sanctions arises only under certain circumstances
  - Must comply with U.S. sanctions when engaging in a transaction with a U.S. touchpoint
  - Can also trigger liability by “causing” a U.S. person to violate OFAC sanctions



# Compliance Obligations: Foreign Subsidiaries

- Most OFAC regulations do *not* apply to foreign subsidiaries, absent some other basis for jurisdiction
  - Many U.S. multinationals apply their U.S./OFAC sanctions compliance program on a global basis, even if not legally required
  - Provides for global consistency and efficiency and helps to prevent inadvertent violations by “facilitating” overseas subsidiaries’ activities
- Two notable exceptions
  - Under the U.S. sanctions programs targeting Cuba and Iran, foreign subsidiaries of U.S. companies are obligated to comply with U.S. sanctions as though they were U.S. persons

# Three Types of Sanctions

Primary Sanctions



1

## Comprehensive Sanctions

- Cuba
- Iran
- North Korea
- Syria
- Crimea
- Donetsk People's Republic ("DNR")
- Luhansk People's Republic ("LNR")

2

## List-Based Sanctions

- Blocking Sanctions
- Sectoral Sanctions

3

## Secondary Sanctions

- Iran
- Russia
- North Korea
- Syria
- Hong Kong
- Terrorism

# Prohibited Parties

## OFAC's 50% Rule

- Restrictions apply to majority-owned entities
- Blocking and sectoral sanctions apply to entities that are owned 50% or more, in the aggregate, by one or more sanctioned parties
- Measured by ownership, and not control

## 50% Rule ownership aggregation examples:

1. Company A is not on the SDN List, but 67% of its shares are owned by Company B, which is on the SDN List. Company A is a blocked party and subject to the same restrictions as Company B.
2. Company C is owned 25% by Company D and 30% by Company E. Companies D & E are on the SDN List. Company C is a blocked party.
3. Company F is owned 45% percent by Company G. Company G is an SDN. Company G controls a majority of Company F's Board of Directors and is the largest shareholder. Company F is not subject to sanctions, but is a risky party.

# KEY CONCEPTS IN U.S. EXPORT CONTROLS

02

# The Rules

- U.S. Statutes
  - AECA
  - ECRA
  - IEEPA
  - TWEA
  - Others
- Executive Orders
- Regulations
- Denial Orders
- Licenses and Exemptions
- Advisory Opinions
- FAQs



# U.S. Department of State

## Directorate of Defense Trade Controls (DDTC)

- International Traffic in Arms Regulations (ITAR)
- Regulate the temporary import, export, reexport, and transfer of defense articles; the provision of defense services to non-U.S. persons; and the brokering of defense articles and defense services
- Defense articles and services are described on the U.S. Munitions List (USML)



# ITAR-Controlled Items and Conduct

- Items and conduct that are **ITAR-controlled** include:
  - All items (referred to as “defense articles”) and services described on the U.S. Munitions List, including technical data
  - Brokering of U.S. and foreign defense articles, including by foreign persons in the U.S. and U.S. persons and their subsidiaries abroad
  - Provision by U.S. persons of defense services to non-U.S. persons, wherever located
- Controls “**follow the item**”
  - Temporary imports to the U.S.
  - Exports
  - Reexports
  - In-country transfers
  - Including when incorporated in non-defense articles
- Certain controls also **follow U.S. persons** (e.g., brokering, defense services)
- Export controls generally apply to all **parties** to a **transaction**
  - Who is a party and what constitutes a transaction is **elastic**

# U.S. Department of Commerce

## Bureau of Industry and Security (BIS)

- Export Administration Regulations (EAR)
- Regulate exports/reexports of nearly all items except ITAR-controlled and certain nuclear energy items:
  - Commodities, software, and technology
  - Includes “dual-use” items (i.e., items that have both civil and military applications) and some military items
- Items “subject to the EAR”
- U.S. person services controls





# Items Subject to the EAR

- Items “**subject to the EAR**” include:
  - All items located in the United States
  - All U.S.-origin items wherever located
  - Foreign-made items incorporating more than a *de minimis* amount of controlled U.S.-origin content
  - Foreign-made items that are the direct product of certain U.S.-origin technology and software or major components that are the direct product of certain technology and software
- Export controls “**follow the item**”
  - Exports
  - Reexports
  - In-country transfers
- Certain controls also **follow U.S. persons**
- Export controls generally apply to all **parties** to a **transaction**
  - Who is a party and what constitutes a transaction is **elastic**

# Compliance Obligations

- **U.S. Persons**
  - U.S. persons include citizens and permanent residents of the United States, entities organized under U.S. state or federal law (including their foreign branches), and any person in the United States
  - Must comply with U.S. export controls at all times and globally, or else face potential civil and criminal liability
- **Non-U.S. Persons**
  - Must comply with U.S. export controls at all times and globally, or else face potential civil and criminal liability
  - Can also trigger liability by causing a violation, or supporting others in their violation, of U.S. export controls

# Authorizations for Exports

Most exports fall into three broad categories:

1

## No License Required

for exports for which no license is required to the final destination, or for the end use/end user, or is not subject to the EAR;

2

## General License or License Exception Applies

where export authorization is required, a general license or “license exception” can apply, and therefore no license is needed if the exporter relies on and satisfies all the conditions of the general license or exception; or

3

## Export License Required

which means BIS written authorization is needed prior to exporting.

# Export Licensing

- BIS **export authorization requirements** can depend on:
  - What is the item and how is it controlled?
  - Where is it going?
  - Who is the end user?
  - What is the intended end use?
  - Whether a U.S. person is providing certain kinds of services
    - Application of know-how by U.S. persons abroad is a kind of export
    - Growing list of U.S. person services prohibitions that apply regardless whether items subject to U.S. export controls are involved in the services
  - Whether an item being exported, reexported, or transferred has been involved in an unlawful transaction

# EAR Prohibitions

1. General Prohibition One — Export/reexport of controlled items to listed countries
2. **General Prohibition Two — Reexport and export from abroad of foreign-made items incorporating more than a *de minimis* amount of controlled U.S. content**
3. **General Prohibition Three — Foreign direct product (FDP) rules**
4. General Prohibition Four — Engaging in actions prohibited by a denial order
5. **General Prohibition Five — Export or reexport to prohibited end-uses/end-users**
6. General Prohibition Six — Export or reexport to embargoed destinations
7. General Prohibition Seven — Support of proliferation activities and certain military intelligence end uses and end users
8. General Prohibition Eight — In transit shipments and items to be unladen from vessels or aircraft
9. General Prohibition Nine — Violation of any order, terms, and conditions
10. **General Prohibition Ten — Proceeding with transactions with **knowledge** that a violation has occurred or is about to occur**
  - **Includes not only positive knowledge that the circumstance exists or is substantially certain to occur, but also an awareness of a high probability of its existence or future occurrence.**
  - **Such awareness is inferred from evidence of the conscious disregard of facts known to a person and is also inferred from a person's willful avoidance of facts.**

# REGULATORY TRENDS

03

# Statute of Limitations

- **U.S. Sanctions**
  - 21st Century Peace Through Strength Act (April 24, 2024)
  - Extends the statute of limitations for sanctions violations from 5 years to **10 years**
  - Applies to **civil and criminal** proceedings
- **U.S. Export Controls**
  - **5-year** statute of limitations
  - Applies to **civil and criminal** proceedings
  - No indication that statute of limitations will be extended
- **Practical Implications**
  - Recordkeeping requirements, starting in March 2025
  - Lookback period for investigations
  - Civil monetary penalties and voluntary self-disclosures
  - Due diligence for mergers, acquisitions, and investments
  - Representations and warranties

# Supreme Court: *Loper Bright*

- *Loper Bright Enterprises v. Raimondo*
  - Overruled *Chevron v. Natural Resources Defense Council*
  - Courts were previously required to defer to agencies' **reasonable** interpretation of **ambiguous** statutory terms
  - Courts now must **independently interpret** statutes without deference to an agency's reading of the law
- **Practical Implications**
  - Resets balance of power between:
    - Courts and agencies
    - Agencies and challengers of agency action
  - More difficult for government agencies to win cases turning on statutory-interpretation questions
  - Does not necessarily unsettle prior cases relying on *Chevron*
  - Courts likely to continue deferring to the Executive in the realm of foreign affairs, including sanctions and export controls



# Supreme Court: *Jarkesy*

- *SEC v. Jarkesy*
  - Held that the Seventh Amendment to the U.S. Constitution requires the SEC to sue in **federal court**, not an in-house **administrative court**, when seeking civil penalties for fraud
  - Defendants in such proceedings are entitled to an Article III judge and a jury
- **Practical Implications**
  - Requiring the SEC to bring enforcement actions in federal court will afford defendants access to a neutral arbiter, the rules of evidence and civil procedure, and other procedural protections
  - If an agency seeks monetary penalties on a ground that resembles an action at common law, the Seventh Amendment presumptively requires the agency to proceed in federal court
  - Litigants may challenge administrative enforcement of other federal statutes by **other agencies**, including OFAC and BIS

# Interagency Collaboration

- The **Disruptive Technology Strike Force**—including the U.S. Department of Justice (DOJ), BIS, the Federal Bureau of Investigation, Homeland Security Investigations, and regional U.S. Attorneys' Offices—targets criminal violations of export control laws
- Frequent publication of **joint guidance** documents, including:
  - BIS and the Financial Crimes Enforcement Network (FinCEN) requesting that financial institutions report suspicious transactions related to potential violations of export controls on Russia or the EAR generally
  - Five U.S. Government agencies describing sanctions and export control evasion in the maritime transportation industry and announcing an expectation to “know your cargo”
- Suggests that going forward the United States is likely to continue taking a **whole-of-government approach** to countering sanctions and export control evasion
- Collaboration among agencies will hopefully portend a more unified approach which could make compliance more straightforward

# International Collaboration

- The United States and its allies and partners have joined together to limit Russian sanctions and export control evasion
  - **REPO Task Force**: Allied finance and justice ministries are sharing information in support of joint action on sanctions, asset freezing, asset seizure, and criminal prosecution
  - **Five Eyes**: Australia, Canada, New Zealand, the United Kingdom, and the United States have extended their intelligence-sharing partnership to include coordinating on export control enforcement
  - **Common List of High-Priority Items**: The United States, the European Union, the United Kingdom, and Japan publish a common list of items deemed especially high risk for diversion due to their potential use in Russian weapons systems
- International collaboration now increasingly extends beyond Russia
  - In September 2024, BIS announced the creation of a new **License Exception Implemented Export Controls (IEC)** to recognize and reward countries who impose similar export controls with easier access to items that enable the development of emerging technologies

# ENFORCEMENT TRENDS

04

# Sanctions and Export Control Enforcement

- **Civil and criminal penalties available**
  - No action / cautionary letters
  - Civil monetary penalties
  - Imprisonment for willful violations
- **Corporate and individual liability**
- **Most violations can be charged on a strict liability basis**
  - Some prohibitions have knowledge requirements
  - In practice, enforcement often occurs when evidence of negligence, recklessness, or willfulness



# OFAC Guidelines

## Base Penalty – Calculated per Transaction

- Egregious?
- Voluntarily self-disclosed?

## Mitigating and Aggravating Factors

- Willful or reckless
- Awareness of conduct
- Management involvement
- Pattern of conduct and repeat violations
- Harm to sanctions program objectives
- Volume of transactions
- Size and sophistication of violating person
- Existence and adequacy of compliance program
- Remedial response
- Cooperation

### BASE PENALTY MATRIX

		Egregious Case	
		NO	YES
Voluntary Self-Disclosure	YES	(1) One-Half of Transaction Value (capped at <u>lesser</u> of \$184,068 or one-half of the applicable statutory maximum per violation)	(3) One-Half of Applicable Statutory Maximum
	NO	(2) Applicable Schedule Amount (capped at <u>lesser</u> of \$368,136 or the applicable statutory maximum per violation)	(4) Applicable Statutory Maximum

Civil monetary penalties available under IEEPA include \$368,136 or twice the value of the underlying transaction, whichever is greater

# OFAC Monetary Penalties

## Civil Penalties

	Total Penalties	# Actions
2014	\$1,205,225,807	22
2015	\$599,705,997	15
2016	\$21,609,315	9
2017	\$119,527,845	16
2018	\$71,510,561	7
2019	\$1,289,027,059	26
2020	\$23,565,657	16
2021	\$20,896,739	20
2022	\$42,664,006	16
2023	\$1,541,380,594	17
2024	\$31,730,943	4

## Significant Fines

- OFAC monetary penalties only tell a portion of the story
- Other U.S. regulators and enforcement agencies such as the DOJ, SEC, NYDFS and others may also impose penalties, disgorgement, and forfeiture requirements
- In 2014, a major European bank's total penalty calculation to settle its sanctions issues with the United States totaled nearly \$9 billion

# OFAC Enforcement Trends

## Record-Breaking Penalties

- During 2023, OFAC for the first time ever imposed a combined **\$1.5 billion** in civil monetary penalties
- Although the number of enforcement actions resulting in monetary penalties was unexceptional, the size of those penalties was striking
- Last year, OFAC levied two of the six largest civil penalties in its history, including a **\$508 million** settlement with a global tobacco company and a record-breaking **\$968 million** settlement with a leading cryptocurrency exchange

## Parallel Resolutions

- Multiple cases—including the two largest penalties imposed by OFAC during 2023—involved parallel resolutions with the U.S. Department of Justice and other agencies
- Suggests an increased appetite on the part of the U.S. Government for **civil and criminal enforcement** of U.S. sanctions



# BIS/DDTC Penalties

## BIS Guidelines

### Aggravating Factors

- Willful or reckless
- Awareness of conduct
- Harm to regulatory program objectives
- Failure to disclose a significant apparent violation

### Mitigating Factors

- Remedial response
- Exceptional cooperation
- License likely to be approved

### General Factors

- Individual characteristics (e.g., size and sophistication, volume and value of transactions, regulatory/criminal history)
  - Criminal history now extends beyond export-related violations, and includes resolutions other than guilty pleas (e.g., NPA, DPA)
- Existence and adequacy of compliance program

## BIS Penalties

### BASE PENALTY MATRIX

Voluntary self-disclosure?	Egregious case?	
	NO	YES
YES	(1) Up to One-Half of the Transaction Value	(3) Up to One-Half of the Applicable Statutory Maximum.
NO	(2) Up to the Transaction Value	(4) Up to the Applicable Statutory Maximum.

Civil monetary penalties available under ECRA include \$364,992 or twice the value of the underlying transaction, whichever is greater

## DDTC Penalties

- Civil monetary penalties of up to \$1 million+ per violation
- Criminal penalties of up to \$1 million, 20 years' imprisonment, or both, per violation
- Debarment

# BIS Enforcement Trends

## Record-Breaking Penalties

- BIS in April 2023 announced a **\$300 million** civil penalty against two affiliates of a global technology company for allegedly selling hard disk drives to Huawei in violation of U.S. export controls
- Largest standalone administrative penalty in the agency's history
- First action targeting an alleged violation of the **Huawei-specific Foreign Direct Product Rule**—a notoriously complex regulatory provision that expands the scope of U.S. export controls to certain foreign-produced items that are derivative of specified U.S. software and technology

## Benefits of Voluntary Self-Disclosures

- North American affiliate of a Germany-based company voluntarily self-disclosed to DOJ an employee's diversion of chemical products to China
- Company self-disclosed one week after retaining external counsel to conduct an internal investigation
- Employee and a co-conspirator entered guilty pleas
- Company received a **declination**
- No monetary penalty, disgorgement, forfeiture, or restitution was required

# WEIGHING THE DECISION TO SELF-DISCLOSE


05

# Evolution of BIS Enforcement Policy



- In September 2024, BIS announced the publication of a final rule updating its policies regarding **voluntary self-disclosures (VSDs)**
- Codifies in the EAR a series of policy changes that were first articulated in **memoranda** issued by BIS beginning in 2022
- Seeks to encourage voluntary disclosures by:
  - Streamlining self-disclosure of minor or technical violations
  - Facilitating corrective action that might otherwise be prohibited
  - Prioritizing “significant” violations by establishing a **dual-track process** for VSD submission and processing
  - Treating failure to disclose significant apparent violations as an **aggravating factor**
  - Enhancing BIS’s **discretion in assessing penalties**
  - Incentivizing compliance-minded firms to report violations committed by other firms or competitors

# Evolution of DOJ Enforcement Policy



**Department of Justice**

---

Updated March 7, 2024  
[www.justice.gov](http://www.justice.gov)

NSD  
(202) 514-2007

**NSD ENFORCEMENT POLICY FOR BUSINESS ORGANIZATIONS<sup>1</sup>**

**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.

## Criminal Enforcement

- U.S. Department of Justice's National Security Division (NSD) handles criminal enforcement of U.S. sanctions and export control 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 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 sanctions and export controls carry penalties of up to **\$1 million**, imprisonment up to **20 years**, and criminal forfeiture

# DOJ National Security Division Expectations

Prompt disclosure directly to NSD of all **potentially criminal** violations of the Arms Export Control Act, the Export Control Reform Act, or the International Emergency Economic Powers Act, 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

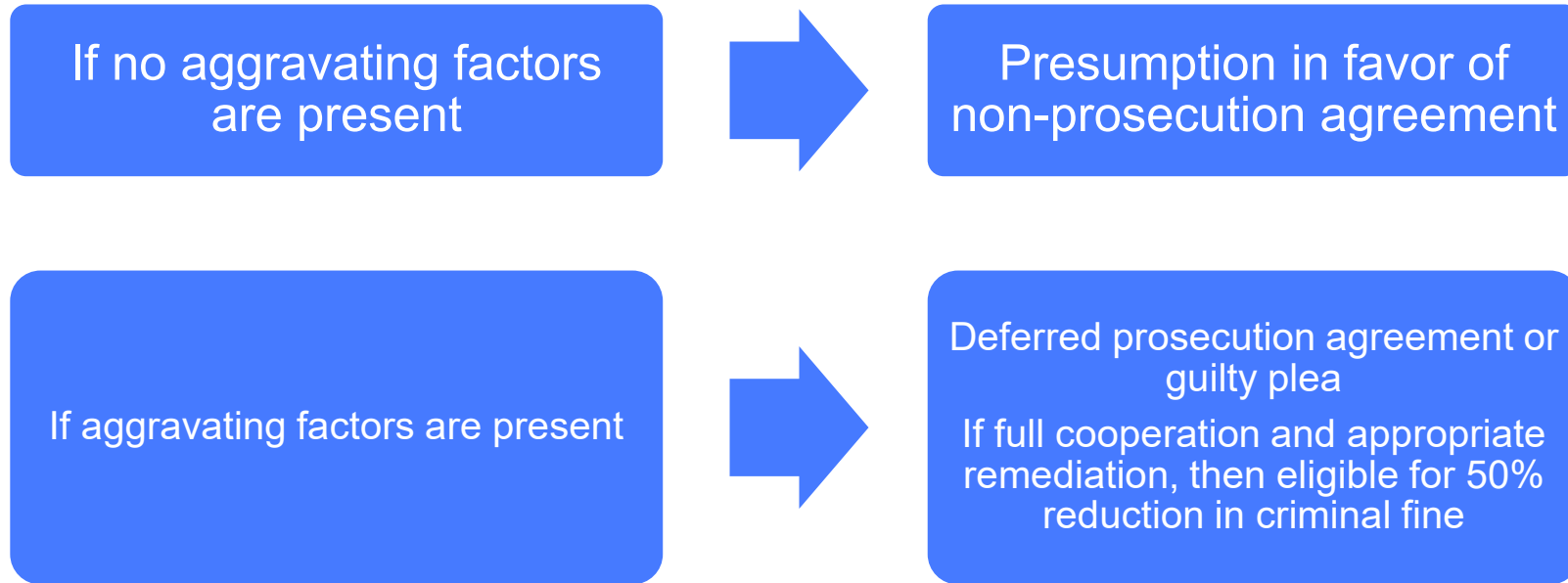
## Remediation

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.



# CONDUCTING SUCCESSFUL INVESTIGATIONS

06

# Conducting a Sanctions or Export Control Investigation: **Overview**

Increased focus by NSD on sanctions and export controls counsels in favor of a swift, thorough, and formal investigation of potential criminal sanctions or 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



# QUESTIONS?

# Upcoming Programs – Fall White Collar Webcast Series

Date and Time	Program	Registration Link
<p style="text-align: center;">Tuesday, October 22, 2024 12:30 PM – 1:30 PM ET 9:30 AM – 10:00 AM PT</p>	<p><b>A New Era of Environmental Criminal Enforcement</b> Presenters: Michael Diamant, Rachel Levick, Stacie Fletcher, David Fotouhi</p>	<p style="text-align: center;"><a href="#"><u>Event Details</u></a></p>
<p style="text-align: center;">Thursday, October 24, 2024 12:00 PM – 1:00 PM ET 9:00 AM – 10:00 AM PT</p>	<p><b>SEC Enforcement Update</b> Presenters: Mark Schonfeld, David Woodcock, Tina Samanta</p>	<p style="text-align: center;"><a href="#"><u>Event Details</u></a></p>
<p style="text-align: center;">Thursday, November 7, 2024 1:00 PM – 2:30 PM ET 10:00 AM – 11:30 AM PT</p>	<p><b>False Claims Act Enforcement in the Life Sciences and Health Care Sectors</b> Presenters: John Partridge, Jonathan Phillips, Katlin McKelvie, Jim Zelenay</p>	<p style="text-align: center;"><a href="#"><u>Event Details</u></a></p>
<p style="text-align: center;">Wednesday, November 13, 2024 3:00 PM – 4:00 PM ET 12:00 PM – 1:00 PM PT</p>	<p><b>Government Investigations into AI Systems</b> Presenters: Eric Vandevelde, Chris Whittaker, Poonam Kumar</p>	<p style="text-align: center;"><a href="#"><u>Event Details</u></a></p>

**GIBSON DUNN**

**Appendix:**

**CONDUCTING  
SUCCESSFUL  
INVESTIGATIONS**

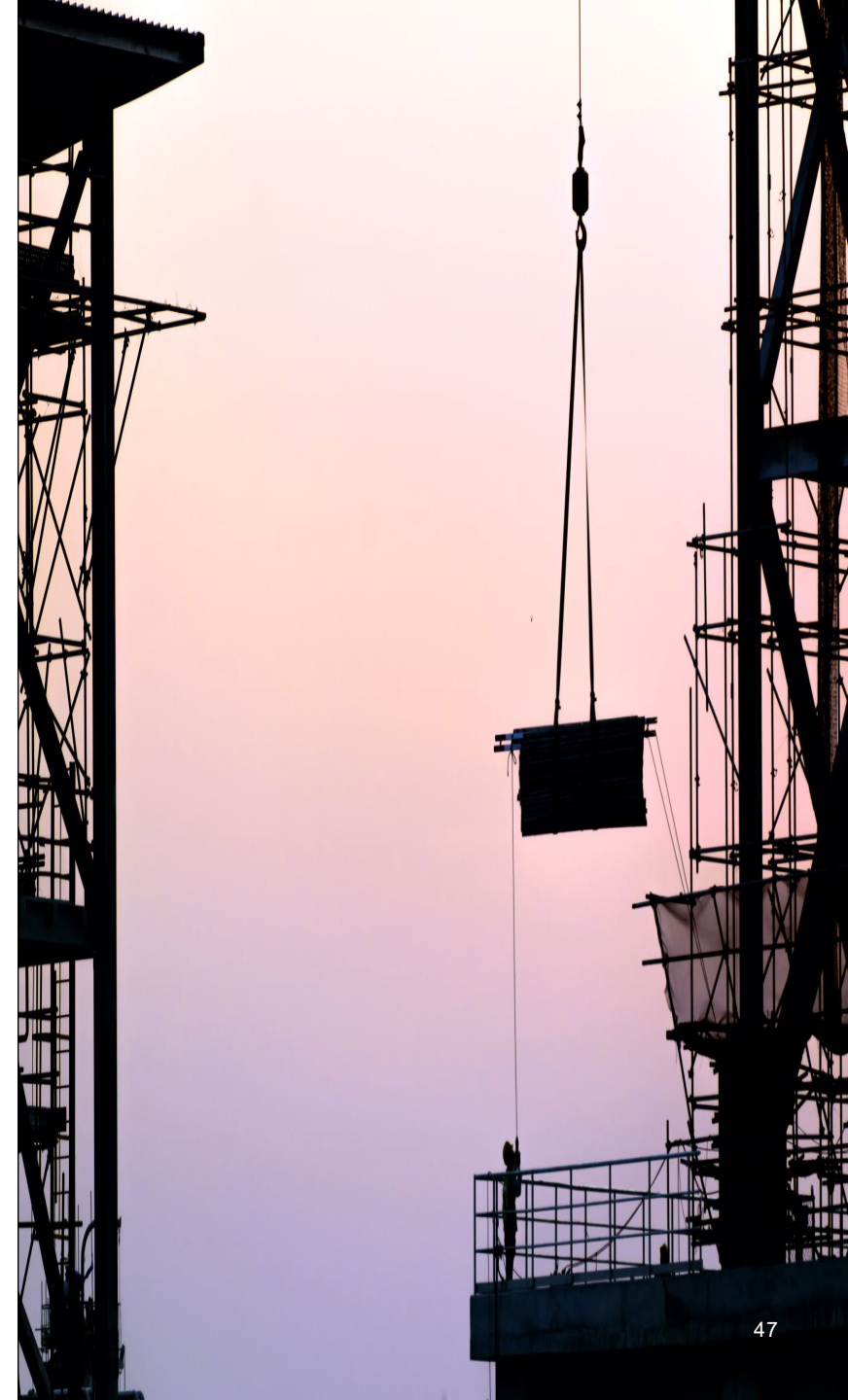
# Conducting a Sanctions or Export Control Investigation: **First Steps**

## 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 vs. external counsel, attorneys vs. non-attorneys)
- Agencies to which disclosure is made
- Timing and sequencing of any disclosure



# Conducting an Investigation

## Protecting Privilege

- Any sanctions or export control allegation or violation with any level of criminal flavor should be investigated at the direction of (internal 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
- 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” markings 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





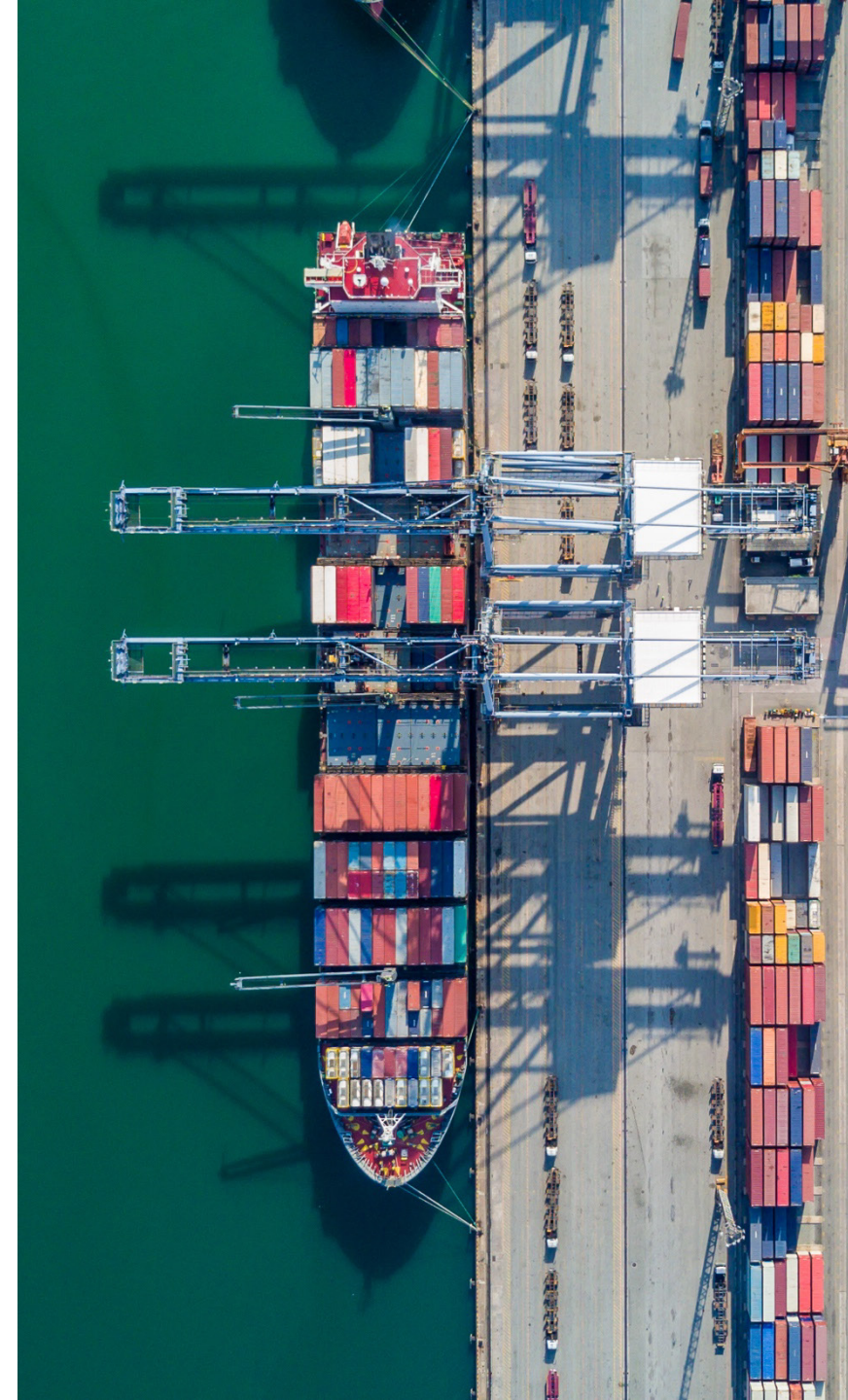
# Conducting an Investigation

## 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 Investigation

## 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 (e.g., ephemeral messages)
- Be mindful of foreign laws and regulations that could impact how information is collected (e.g., GDPR, PRC data privacy and state secrets)

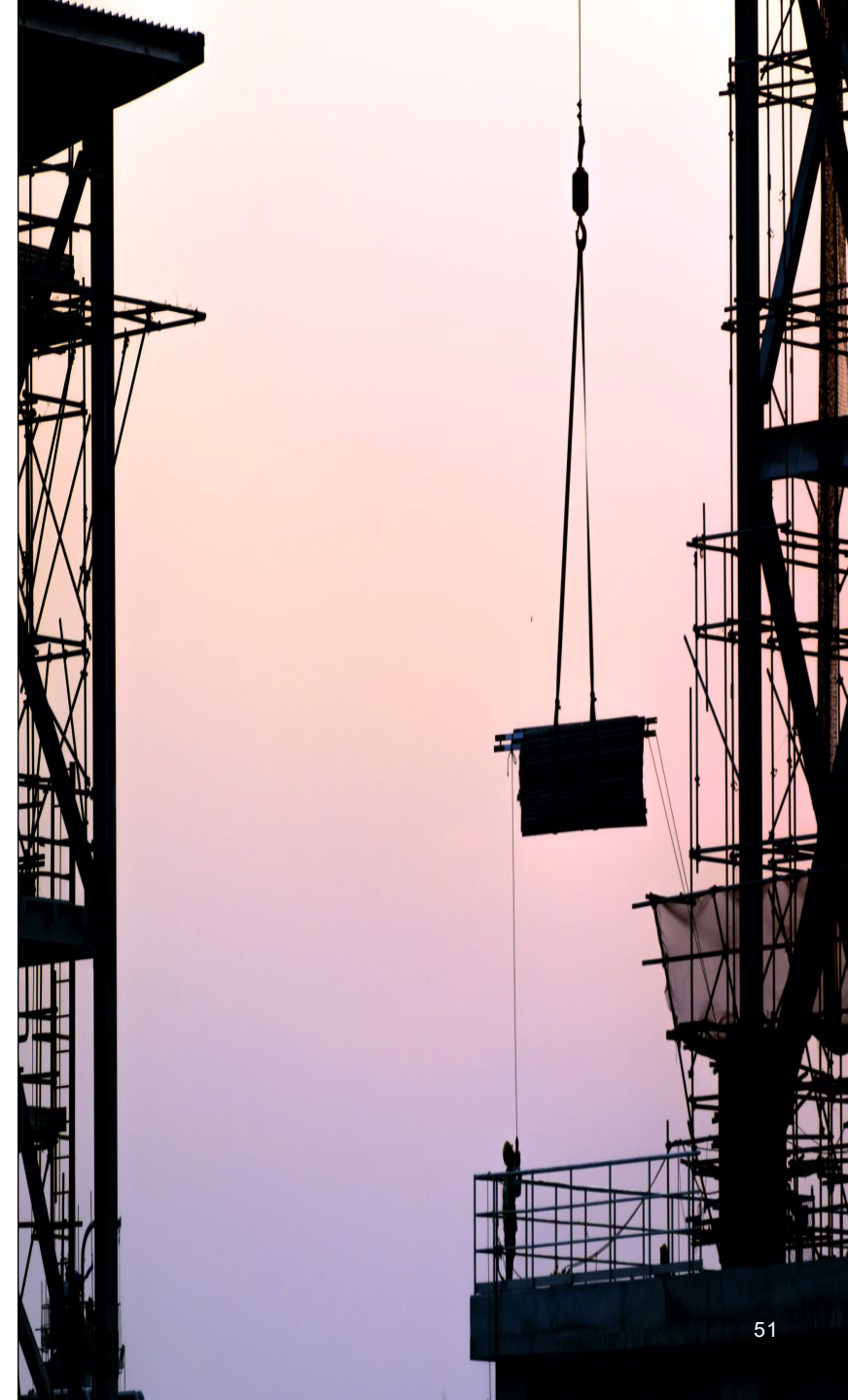


# Conducting an Investigation

## 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 vs. 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 Investigation

## 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 vs. written submissions
- Consider joint vs. separate briefings for multi-agency enforcement actions
- Privilege (and waiver) will be a thorny consideration if 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

