September 2021

NATIONAL SECURITY ENFORCEMENT

GIBSON DUNN

MCLE Credit Information

Most participants should anticipate receiving their certificate of attendance via email approximately one month following the webcast.

Virginia Bar Association members should anticipate receiving their certificate of attendance two months following the webcast.

Please direct all questions regarding MCLE to CLE@gibsondunn.com

Today's Presenters

David P. Burns

Zainab Ahmad

Robert K. Hur

Adam M. Smith

Courtney M. Brown

National Security Enforcement at DOJ

Critical to successful advocacy in the national security space is understanding strategic priorities and trends in enforcement. While counterterrorism consistently has remained a top priority for DOJ across administrations, there has been a renewed focus on counterintelligence activities and great power competition at DOJ and throughout the nation's national security apparatus.

"[T]he lawyers, agents, and analysts at the Department of Justice work closely with our colleagues across the national security community to detect and disrupt terrorist plots, to prosecute suspected terrorists, and to identify and implement the legal tools necessary to keep the American people safe."

- Attorney General, 2012

"The [People's Republic of China's] economic aggression and theft of intellectual property comes with immense costs. The [DOJ] will continue to use our full suite of national security tools to combat the threat posed by theft directed and encouraged by the PRC."

- Attorney General, 2020

Department of Justice Strategic Goals

For the 2014-2018 period, the three strategic goals of the Department of Justice were to:

- **Goal 1:** Prevent Terrorism and Promote the Nation's Security Consistent with the Rule of Law
- **Goal 2:** Prevent Crime, Protect Rights of the American People, and Enforce Federal Law
- **Goal 3:** Ensure and Support the Fair, Impartial, Efficient and Transparent Administration of Justice at the Federal, State, Local, Tribal and International Levels

For the 2018-2022 period, the four strategic goals of the Department of Justice are to:

- **Goal 1:** Enhance National Security and Counter the Threat of Terrorism
- **Goal 2:** Secure the Borders and Enhance Immigration Enforcement and Adjudication
- **Goal 3:** Reduce Violent Crime and Promote Public Safety
- **Goal 4:** Promote Rule of Law, Integrity, and Good Government

(DOJ Strategic Plan FY 2014-2018; DOJ Strategic Plan FY 2018-2022)

National Security Enforcement at DOJ

National Security enforcement at DOJ has included the following priorities:

- Counterterrorism & Terrorism Financing
- Sanctions & Export Controls
- Theft of Intellectual Property & Economic Espionage
- Cyber Intrusion
- Foreign Agents Registration Act ("FARA")
- Foreign Investment in the United States

We expect a focus on China—through the China Initiative or a similar, rebranded effort—to remain a consistent enforcement priority in the coming years.

National Security Division - Overview

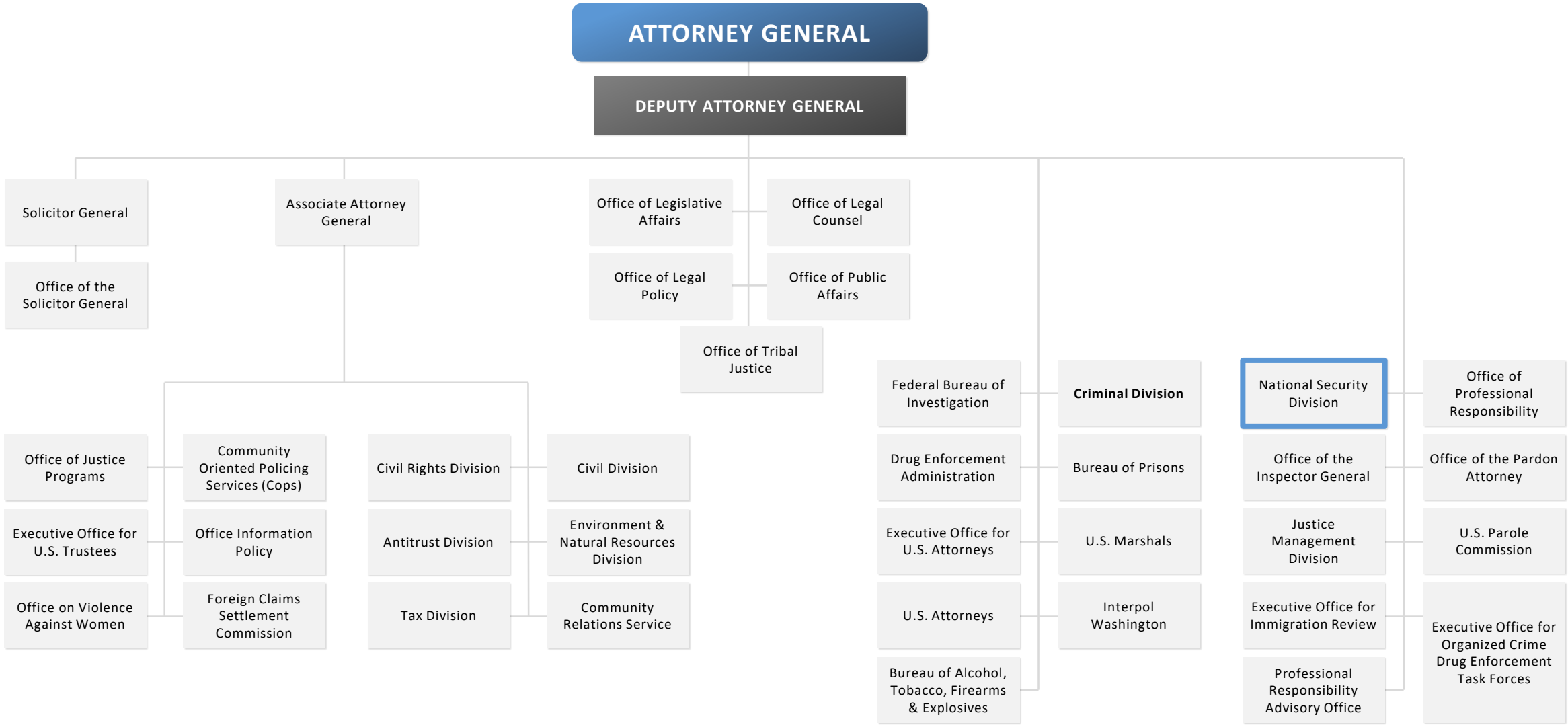
The **National Security Division (NSD)** was created in March 2006 by the USA PATRIOT Reauthorization and Improvement Act, consolidating the DOJ's primary national security operations: the former **Office of Intelligence Policy and Review** and the **Counterterrorism** and **Counterintelligence and Export Control Sections** of the Criminal Division. The new **Office of Law and Policy** and the **Executive Office**, as well as the **Office of Justice for Victims of Overseas Terrorism** (which previously operated out of the Criminal Division) complete NSD. NSD commenced operations in September 2006.

NSD's organizational structure is designed to ensure greater coordination and unity of purpose between prosecutors and law enforcement agencies, on the one hand, and intelligence attorneys and the Intelligence Community, on the other.

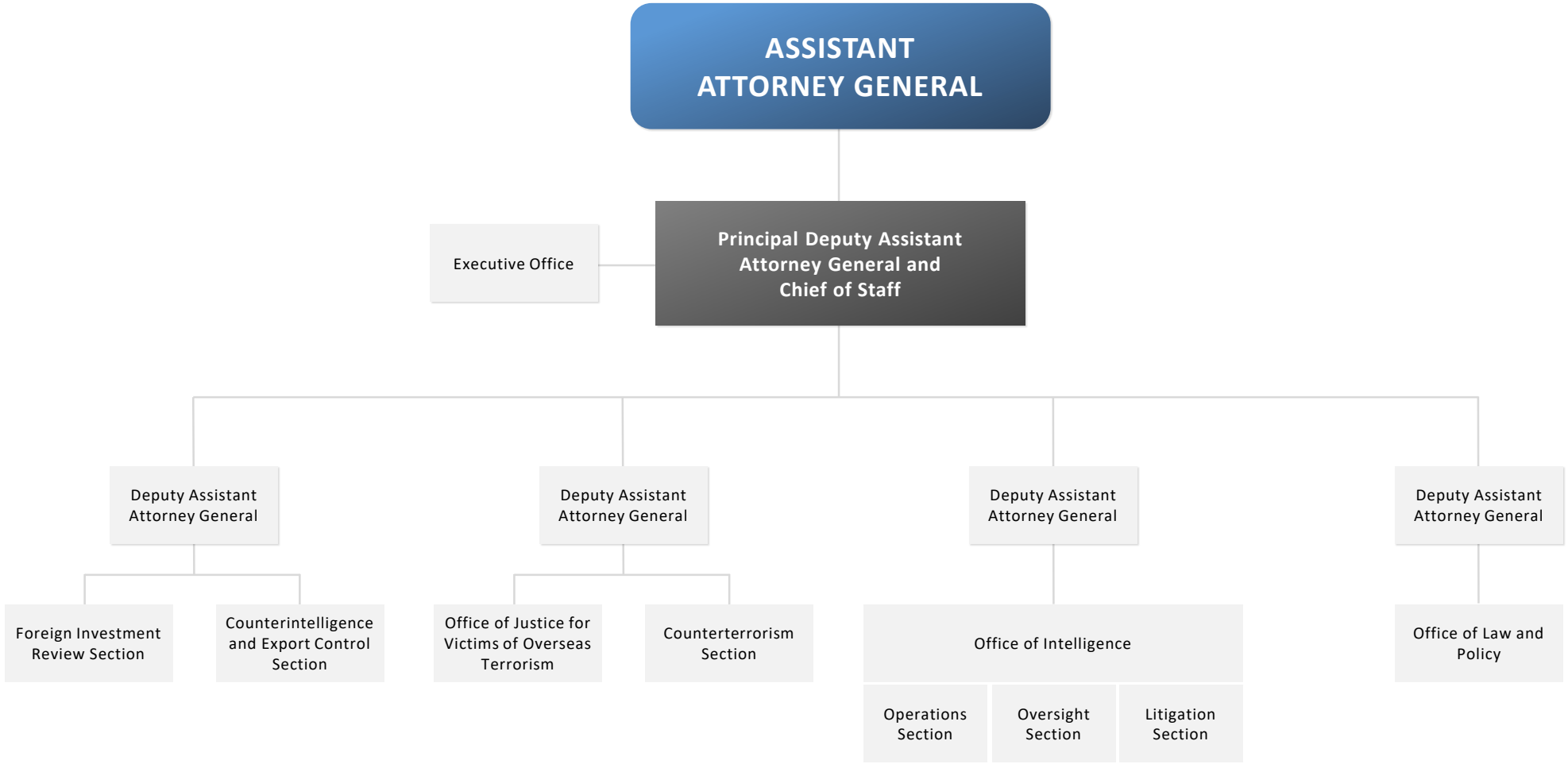
About the Division, justice.gov/nsd/about-division

The National Security Division' mission is to implement the Department's highest priority: protect the United States from threats to our national security by pursuing justice through the law.

National Security Division - Organization



National Security Division - Organization



Counterterrorism and Terrorism Financing

- **Material Support to Foreign Terrorist Organizations:** 18 U.S.C. § 2339B prohibits knowingly providing material support or resources to a foreign terrorist organization. Section 2339B also requires financial institutions that become aware of such funds to retain and report them to the Treasury Department.

- **Financing of Terrorism:** 18 U.S.C. § 2339C prohibits those that willfully provide or collect funds to carry out offenses, inter alia, that cause "death or serious bodily injury to a civilian, or to any other person not taking part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context is to intimidate a population, or compel a government or an international organization to do or to abstain from doing any act."

- Disrupting and prosecuting material support for terrorism and traditional funds transfers to terrorist groups remains a DOJ priority. For example:

  - In 2020, DOJ charged a New Jersey woman for sending money to a Syria-based al-Nusra Front fighter via Western Union, using an intermediary to conceal the source of funds.

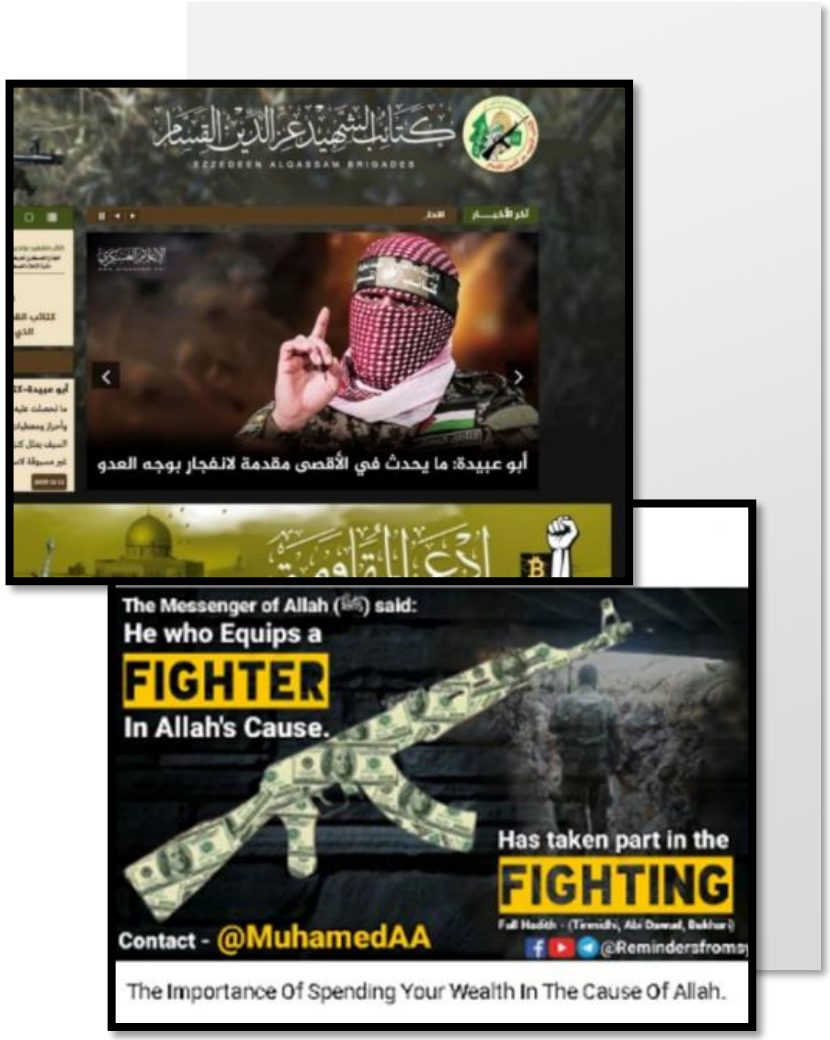
  - In 2019, an Indiana woman pleaded guilty to a concealment of terrorism financing charge for transporting more than $30,000 in cash and gold from the United States to a safety deposit box in Hong Kong for use by her relatives to join ISIS.

Counterterrorism and Terrorism Financing

Recent years have witnessed a focus on the use of cryptocurrency and other online means to support terrorist groups.

- In a landmark event in August 2020, DOJ announced actions to seize cryptocurrency and dismantle online fundraising campaigns associated with the al-Qassam Brigades (the military wing of Hamas), Al Qaeda, and ISIS. The seizure was the largest ever of terrorist organizations' cryptocurrency accounts, which involved Bitcoin fundraising and money laundering efforts via social media and fake websites.

- Similarly, in October 2020, DOJ seized "aletejahtv.com" and "kataibhezbollah.com," two websites used by SDN and Foreign Terrorist Organization Kata'ib Hizballah.



Counterterrorism and Terrorism Financing

Cryptocurrency Enforcement Framework

- This enhanced focus on new financing methods is evident in "**Cryptocurrency: Enforcement Framework**" announced by DOJ last year, which sets out the threat overview, regulations and authorities, and ongoing challenges and future strategies associated with criminal use of cryptocurrency.

- As the Task Force notes: "Crime has been expanding beyond national borders for years, but blockchain takes this globalization to another level. Parties conduct transactions between continents in a matter of minutes, and the digital infrastructure of the blockchain itself almost always transcends territorial boundaries."

- In response to such challenges the Framework suggests: "Consistent with its mission to protect public safety and national security, the Department of Justice will continue its aggressive investigation and prosecution of a wide range of malicious actors, including those who use cryptocurrencies to commit, facilitate, or conceal their crimes."

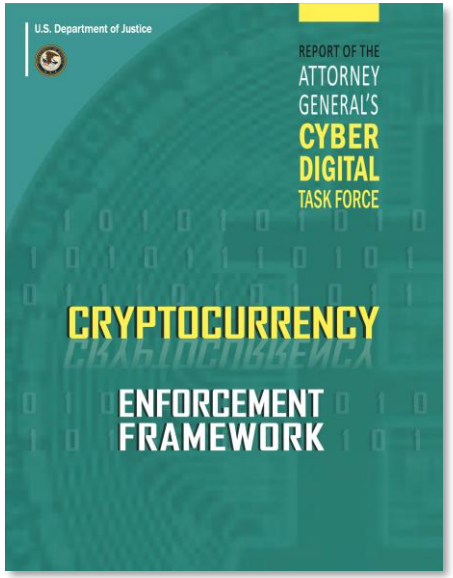


Image Source:
https://www.justice.gov/archives/ag/page/file/1326061/download

Sanctions and Export Controls

- NSD has the authority to investigate and prosecute sanctions and export controls violations under the Arms Export Control Act (AECA), 22 U.S.C. § 2778; the Export Control Reform Act (ECRA), 50 U.S.C. § 4801; and the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. § 1705.
- Criminal violations of the sanctions and export controls laws generally involve willful conduct.
- The Department of Treasury's Office of Foreign Asset Controls ("OFAC") oversees civil violations of these same authorities.
- The Department of Commerce's Bureau of Industry and Security ("BIS") enforces export controls related to dual use civilian/military items and maintains the Entity List.
- The Department of State's Directorate of Defense Trade Controls ("DDTC") enforces export controls related to military designated items.

Image Source: https://www.internationaltradecomplianceupdate.com/

Sanctions and Export Controls

Enforcement Landscape

Sanctions

U.S. Treasury Department's Office of Foreign Assets Control (OFAC)

Economic and trade sanctions programs prohibit transactions with *certain countries, institutions, and individuals* in order to accomplish foreign policy and national security goals.

Sanctions programs are primarily concerned with the **WHO**.

U.S. Justice Department's National Security Division (NSD)

Has jurisdiction to prosecute sanctions violations where the statute authorizes criminal enforcement.

Export Controls

U.S. Commerce Department's Bureau of Industry and Security (BIS)

Covers dual use military/commercial items.

U.S. State Department's Directorate of Defense Trade Controls (DDTC)

Covers military designed items.

Export control regulations identify items, software, technology and services that may require an export license to transfer out of the U.S.

Export control regulations are primarily concerned with the WHAT.

U.S. Justice Department's National Security Division (NSD)

Has jurisdiction to prosecute export controls violations where the statute authorizes criminal enforcement.

Sanctions and Export Controls

VSD Policy

Under the Export Control and Sanctions Enforcement Policy for Business Organizations, DOJ encourages businesses to voluntarily self-disclose (VSD) export controls and sanctions violations, cooperate with investigations, and timely and appropriately remediate the underlying causes of the violation. Companies that do so, absent aggravating factors, benefit from a presumption they will receive a non-prosecution agreement and not pay a fine.

The policy was revised in 2019 to:

- Provide more clarity concerning the benefits of reporting and the consequences of not reporting;
- Require that a VSD be made to CES to receive its benefits (reporting to a regulator agency—such as DDTC, BIS, or OFAC—will not suffice);
- Bring the policy in line with similar VSD enforcement frameworks, most notably, the Criminal Division's Foreign Corrupt Practices Act (FCPA) policy; and
- Remove the carveout for financial institutions that had existed in the earlier policy.

- Dec. 3, 2019 Speech by NSD PDAAG David Burns

Sanctions and Export Controls

Revised VSD Policy Case Study: SAP SE

On April 29, 2021, SAP SE ("SAP"), a German software corporation, entered into an non-prosecution agreement with DOJ and agreed to disgorge $5.14 million, the first such action to occur under the revised VSD policy.

SAP voluntarily disclosed export controls and sanctions violations, including 20,000 instances of the provision of U.S.-origin software and technology through cloud servers to Iranian-based end-users.

> "Today's first-ever resolution pursuant to the Department's Export Control and Sanctions Enforcement Policy for Business Organizations sends a strong message that businesses must abide by export control and sanctions laws, but when they violate those laws, there is a clear benefit to coming to the Department before they get caught. SAP will suffer the penalties for its violations of the Iran sanctions, but these would have been far worse had they not disclosed, cooperated, and remediated. We hope that other businesses, software or otherwise, heed this lesson."
>
> - Assistant Attorney General John C. Demers

- Dec. 3, 2019 Speech by NSD PDAAG David Burns

Sanctions and Export Controls

Other Recent Prosecutions

Additional recent prosecutions show the wide range of sanctions and export controls enforcement targets, spanning geographic regions and industry types. Also notable are the large fines—often eclipsing $1 billion—that accompany such actions.

Huawei: In a series of superseding indictments in 2019 and 2020, the Chinese telecom giant was charged with theft of intellectual property, sanctions violations, bank and wire, and RICO conspiracy. As alleged by DOJ, the sanctions violative conduct involved "arranging for shipment of Huawei goods and services to end users in sanctioned countries," often through local affiliates using code names for certain jurisdictions—"For example, the code 'A2' referred to Iran, and 'A9' referred to North Korea."

Halkbank: The state-owned Turkish bank was charged in 2019 with fraud, money-laundering and sanctions offenses related to Iran. Per the SDNY U.S. Attorney, the sanctions violative conduct involved "Halkbank's systemic participation in the illicit movement of billions of dollars' worth of Iranian oil revenue and was designed and executed by senior bank officials…supported and protected by high-ranking Turkish government officials."

Sanctions and Export Controls

Other Recent Prosecutions

Standard Chartered: In 2019, the bank paid over $1 billion in penalties for conspiracy to violate IEEPA by processing 9,500 financial transactions worth $240 million through U.S. financial institutions for the benefit of Iran. The Criminal Division Assistant Attorney General stated in relation to the announcement of the Deferred Prosecution Agreement: "Today's resolution sends a clear message to financial institutions and their employees: if you circumvent U.S. sanctions against rogue states like Iran—or assist those who do—you will pay a steep price."

Oil Vessel Seizures: In 2020, DOJ announced the disruption and seizure of a fuel shipment from Iran's Islamic Revolutionary Guard Corps bound for Venezuela, the government's largest-ever seizure of fuel shipments from Iran.

Airbus: In 2020, the French aerospace firm paid combined penalties of $3.9 billion to French, UK, and U.S. authorities to resolve foreign bribery and export control charges, including export controls violations under the International Traffic in Arms Regulations ("ITAR"). As David Burns, then serving as Principal Deputy Assistant Attorney General at NSD, explained: "International corruption involving sensitive U.S. defense technology present a particularly dangerous combination."

Foreign Agents Registration Act

Enforcement Trends

- "[B]etween the last major overhaul of the statute in 1966 and 2016, there were only seven criminal prosecutions under the statute. Nearly 30 years had passed between the last civil injunction in 2019 and its predecessor. By 2014, active FARA registrations had declined by 60 percent from their peak in the late 1980s."

- "[Robert Mueller's] Special Counsel's Office undeniably helped reverse that decline by highlighting FARA's relevance to modern challenges of covert foreign influence and injecting adrenaline into the department's enforcement efforts."

  - Dec. 4, 2020 Speech by NSD DAAG Adam Hickey

Criminal liability under FARA attaches to someone who "willfully" fails to register, or willfully makes a false statement in a registration. Criminal investigations are initiated in cases where there are indications that a failure to register was intentional, or that the recipient of a letter of inquiry was acting in bad faith.

Foreign Agents Registration Act

Scope of Agency

- FARA applies to one **"who acts as an agent, representative, employee or servant, or any person who acts in any other capacity at the order, request, or under the direction or control"** of a foreign principal. 22 U.S.C. § 611(c)(1).

- NSD recently issued guidance on the scope of agency under FARA to further clarify who falls within the definition of "an agent of a foreign principal." With particular focus on the "request" element of the definition, NSD offered the following:

- *The ultimate test for agency under FARA is whether it is "fair to draw the conclusion that an individual is not acting independently, is not simply stating his or her own views, but is acting as an agent or alter ego of the foreign principal." ... Although "the exact perimeters of a 'request' under the Act are difficult to locate," and mere persuasion would be insufficient, "the surrounding circumstances will normally provide sufficient indication as to whether a 'request' by a 'foreign principal' requires the recipient to register as an 'agent.'"*

- DOJ guidance concludes that, accordingly, "these circumstances must evince some level of power by the principal over the agent or **some sense of obligation on the part of the agent to achieve the principal's request**." - DOJ, The Scope of Agency Under FARA

Image Source: https://www.justice.gov/nsd-fara

Foreign Agents Registration Act

Lawyer's Exemption

- FARA exempts "[a]ny person qualified to practice law, insofar as he engages or agrees to engage in the legal representation of a disclosed foreign principal before any court of law or any agency of the Government of the United States." 22 U.S.C. § 613(g).
- In 1966, when the lawyer's exemption was added, it carried a proviso: "That for the purposes of this subsection legal representation does not include attempts to influence or persuade agency personnel or officials other than in the course of judicial proceedings, criminal or civil law enforcement inquiries, investigations, or proceedings, or agency proceedings required by statute or regulation to be conducted on the record." *Id.*
- NSD has further clarified when this exemption will apply:
  - **First**, "the attorney's relationship with their principal needs to be transparent, at least to the government officials involved."
  - **Second**, "representation of an individual client in an adjudication of that client's interests is distinguishable from advocacy to change U.S. government policies."
  - **Third**, collateral activities "like public relations work that has a tangential relationship to pending litigation … would fall[] outside the exemption."

Foreign Agents Registration Act

Recent Prosecutions

- **Imad Shah Zuberi:** In 2021, Zuberi was sentenced to 12 years in prison (including the statutory maximum of five years for a FARA offense) and ordered to pay nearly $20 million in restitution and criminal fines for making $1 million in illegal campaign contributions. Zuberi solicited foreign nationals and governments (including Sri Lanka and Saudi Arabia) with claims he could influence U.S. foreign policy, and made contributions to high-level U.S. officials, whom he then lobbied. Zuberi also admitted to submitting false registration statements to advance these efforts.

- **Elliott Broidy:** In 2020, Broidy pleaded guilty to one count of conspiracy to violate FARA after admitting to a covert campaign to influence the U.S. government on behalf of Chinese and Malaysian interests in relation to matters ongoing before DOJ, including the 1Malaysia Development Berhad ("1MDB") scandal.

- **Paul J. Manafort, Jr.:** In 2018, Manafort pleaded guilty to conspiracy to violate FARA, money laundering, and obstruction of justice charges in relation to his failure to register under FARA as an agent of the Government of Ukraine and former Ukrainian President Yanukovych.

- **W. Samuel Patten:** In 2018, Patten pleaded guilty to violating FARA as a result of lobbying and political consulting on behalf of a Ukrainian political party, efforts that included lobbying and public relations campaigns.

Foreign Agents Registration Act

Civil Enforcement Actions

RM Broadcasting: In 2019, a federal judge ordered that RM Broadcasting LLC, a Florida-based company, was acting as an agent of a foreign principal and had to register under FARA. DOJ in a civil suit claimed that RM Broadcasting, which operates "Sputnik Radio" in the Washington, D.C. area, was acting on behalf of a Russian state media enterprise controlled by Vladimir Putin. The Assistant Attorney General for the NSD stated "The American people have a right to know if a foreign flag waves behind speech broadcast in the United States."

Theft of Intellectual Property and Economic Espionage

- **18 U.S.C. § 1831 ("Economic Espionage Act")** prohibits the theft of trade secrets, "intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent." **Section 1832** offers similar prohibitions more generally regarding theft of trade secrets for "the economic benefit of anyone other than the owner."
- Under the **Justice Manual**, the Economic Espionage Act "is not intended to criminalize every theft of trade secrets for which civil remedies may exist under state law" and requires special advisory approval by the NSD AAG.
- When considering to initiate a prosecution under **Sections 1831 or 1832**, the Justice Manual requires consideration of:
  - Scope of criminal activity, including evidence of involvement by a foreign government, foreign agent, or foreign instrumentality
  - Degree of economic injury to the trade secret owner
  - Type of trade secret misappropriated
  - Effectiveness of available civil remedies
  - Potential deterrent value of the prosecution

Theft of Intellectual Property and Economic Espionage

Recent prosecutions under the Economic Espionage Act show a substantial focus on theft of intellectual property by Chinese actors.

- **Chi Lung Winsman Ng:** In February 2021, Chinese businessman Chi Lung Winsman Ng was indicted for conspiring to steal trade secrets from General Electric involving the company's silicon carbide semiconductor technology.

- **Hao Zhang:** In September 2020, Hao Zhang was sentenced to 18 months in prison and nearly half a million dollars in restitution for stealing trade secrets relating to acoustic wave filters used in mobile phones and other devices for consumer and military applications.

- **Hongjin Tan:** In February 2020, Hongjin Tan was sentenced to 24 months in prison for stealing more than $1 billion worth of proprietary information from his employer, a U.S. petroleum company.

"About 80 percent of all economic espionage prosecutions brought by [DOJ] allege conduct that would benefit the Chinese state, and there is at least some nexus to China in around 60 percent of all trade secret theft cases." *– DOJ, Information About the Department of Justice's China Initiative*

- **Shan Shi:** In February 2020, the head of a Houston-based company that was the subsidiary of a Chinese company was sentenced to 16 months in prison for conspiracy to steal trade secrets for pledging to "digest [and] absorb" foam manufacturing technology in the United States.

- **Haitao Xiang:** In November 2019, Haitao Xiang was indicted for trade secrets offenses for the theft of certain farming software from his employer, Monsanto. Xiang was arrested at the airport en route to China with a copy of the company's proprietary algorithm on his person.

Theft of Intellectual Property and Economic Espionage

Recent prosecutions

- Emblematic of this trend is the United Microelectronics Corporation ("UMC") case, in which the Taiwan-based semiconductor foundry pleaded guilty to criminal trade secret thefts and was sentenced to a $60 million fine.

- As part of the deal, UMC agreed to cooperate with the government in the investigation and ultimate prosecution of its co-defendant, Fujian Jinhua Integrated Circuit Co., Ltd., a Chinese state-owned enterprise. The case centered on a conspiracy to steal the trade secrets of American semiconductor company Micron Technology for the benefit of the Chinese government.

- In relation to the case, Deputy Attorney General Jeffrey Rosen stated: "UMC stole the trade secrets of an American leader in computer memory to enable China to achieve a strategic priority: self sufficiency in computer memory production without spending its own time or money to earn it. This prosecution is an example of [DOJ's] successful efforts to defend American companies from those who try to cheat and steal their technology."

Image Source: Maurice Tsai/Bloomberg

Cyber Intrusion

- **18 U.S.C. 1030** generally prohibits knowingly accessing a computer without authorization or exceeding authorized access, including with an intent to defraud or to obtain restricted information related to national defense with "reason to believe that such information so obtained could be used to the injury of the United States or to the advantage of any foreign nation."
  - Additional provisions of Section 1030 prohibit intentionally accessing a computer to obtain financial records and consumer reports or information from any department or agency of the United States or accessing a nonpublic computer of a department of the U.S. government for purposes of conducting fraud.
- Of note, the 2018 indictment of Julian Assange was based on Section 1030 charges that Assange conspired with Chelsea Manning to acquire and transmit classified information from a restricted computer "so that WikiLeaks could publicly disseminate the information on its website."

Image Source: Belga

Cyber Intrusion

Recent prosecutions

Recent actions under Section 1030 demonstrate DOJ's willingness to use the statute to prosecute hacks that affect both the U.S. government and private businesses, including where the subject intrusions overlap with economic espionage and trade secrets theft. For example:

Image Source: Alex Wong/Getty Images

- **Apt 41 Indictments:** In September 2020, DOJ announced charges against five China-based computer hackers for intrusions affecting over 100 victim companies in the United States and abroad, including software development companies, computer hardware manufacturers, telecommunications providers, social media companies, video game companies, non-profits, universities, think tanks, foreign governments and pro-democracy activities in Hong Kong.
- **MSS Hacks:** In July 2020, a federal grand jury indicted two hackers working on behalf of the Guangdong State Security Department and Ministry of State Security for intrusions into hundreds of victim companies, governments, and NGOs, including dissidents and human rights activities in the U.S., Hong Kong and China.
- **North Korean Cyberattacks:** In February 2021, indictments were unsealed against three North Korean computer programmers who conducted a series of cyberattacks aimed at stealing $1.3 billion in money and cryptocurrency from financial institutions and companies.

Ransomware

- Ransomware attacks are on the rise, with malicious actors becoming bolder and increasingly targeting larger organizations with higher ransom demands.
- The issue has become a national security and public health and safety threat, affecting a broad array of public and private systems, ranging from companies to schools, hospitals, police stations, city government, military facilities and critical infrastructure.
- Foreign nation-state adversaries either directly support and cultivate ransomware actors or permit ransomware activities to operate from within their borders with impunity.

> In April 2021, for example, the Treasury Department issued new sanctions against Russia, drawing a connection between Russia's Federal Security Service (FSB) and ransomware actors: "[T]o bolster its malicious cyber operations, the FSB cultivates and co-opts criminal hackers . . . enabling them to engage in disruptive ransomware attacks and phishing campaigns."
>
> - United States Department of the Treasury, "Treasury Sanctions Russia with Sweeping New Sanctions Authority," Press Release, April 15, 2021.

Image Source: Alex Wong/Getty Images

Ransomware

Recent attacks

Earlier this year, the attack on the Colonial Pipeline by the ransomware gang DarkSide captured headlines and led to a run on gas stations and an increase in prices at the pump. Colonial paid $5 million in Bitcoin to the attackers, some of which was recovered by DOJ.

Other recent attacks include:

- CNA Financial Corporation - $40 million
- JSB Foods - $11 million
- Acer - $50 million
- Kaseya VSA (an IT service provider affecting 100 companies) – $70 million

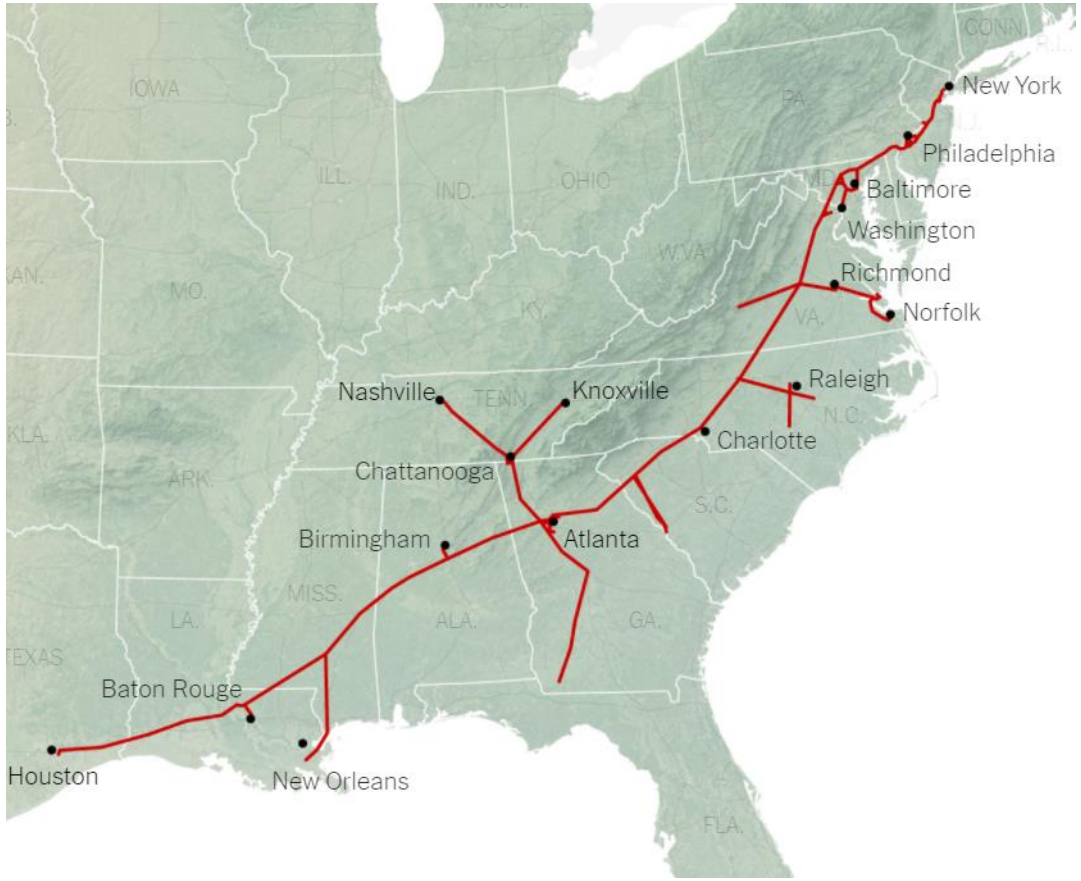


Image Source: NYTimes

Ransomware

Ransomware Victim Cooperation with Law Enforcement

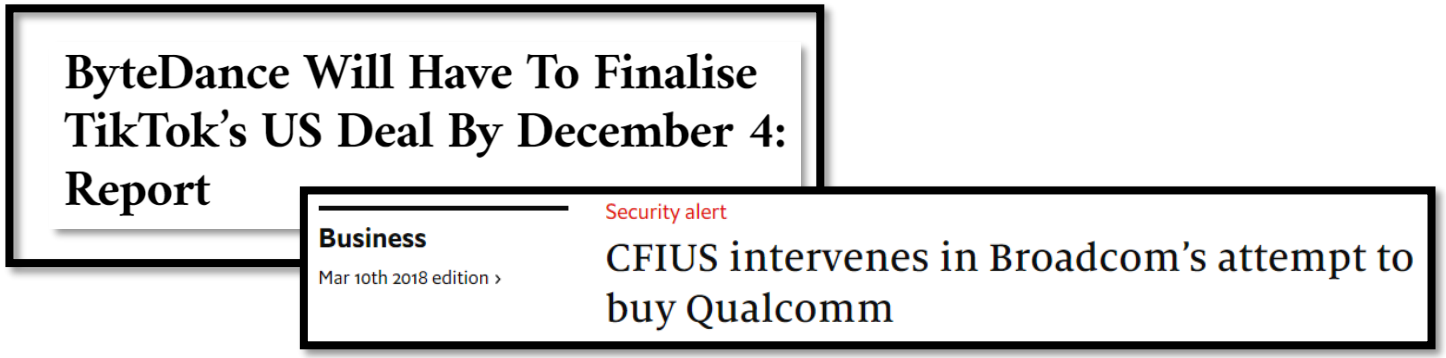
Perceived Cons	Potential Pros
Distraction from core incident response activities	Law enforcement may know ransomware actors and have decryption key
May prompt questions and information requests	Law enforcement may be able to claw back a ransom payment after it is made
Concern that law enforcement could turn attention toward a company's own control failures	Cooperation may mitigate OFAC violations or enforcement
	Cooperation supports an important narrative for regulators, shareholders, and other stakeholders

Image Source: USA Today

CFIUS

Background

- **CFIUS** is an inter-agency committee authorized to review the national security implications of foreign direct investment in the United States.
- CFIUS is authorized to **block** transactions that fall within its jurisdiction or **impose measures to mitigate** any threats to U.S. national security.
- The Committee was established in 1975, reformed in 2007, and operates pursuant to section 721 of the Defense Production Act of 1950, as amended and as implemented by Executive Order 11858, as amended, and regulations at 31 C.F.R. Parts 800-802.



CFIUS

FIRRMA

- Historically, CFIUS only had jurisdiction to review, block, or impose mitigation measures on transactions that could result in a foreign person acquiring control of a U.S. business.
- In 2018, Congress passed and President Trump signed the Foreign Investment Risk Review and Modernization Act ("**FIRRMA**") to modernize the committee and expand its jurisdiction. FIRRMA was widely supported as a tool to protect U.S. technological and military advantages. The rules were finalized and came fully into force in 2020.
- FIRRMA expanded the scope of transactions subject to the Committee's review to include certain foreign non-controlling (equity) investments in U.S. businesses that deal with **critical technology, critical infrastructure, or the sensitive personal data** of U.S. citizens ("**TID**" businesses).

Permanent Member Agencies

There are nine permanent Member Agencies in the Committee

Chair, Treasury

Commerce

Defense

USTR

OSTP

Energy

Homeland Security

State

Justice

In addition, there are five Observer Agencies—CEA, HSC, NEC, NSC, and OMB.

Other agencies may be added for specific reviews.

DOJ Role and Team Telecom

- The **Foreign Investment Review Section** ("**FIRS**") within NSD is responsible for the following portfolios at DOJ:
  - **First**, FIRS manages the Committee for the Assessment of Foreign Participation in the U.S. Telecommunications Services Sector (informally known as Team Telecom) on behalf of its chair, the Attorney General.
  - **Second**, FIRS represents DOJ on CFIUS.
  - **Third**, FIRS monitors compliance with agreements with DOJ or orders that mitigate concerns arising from prior CFIUS or Team Telecom cases and related national security programs.
- In April 2020, President Trump issued the "Executive Order on Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector," which formalized the role of Team Telecom and imposes certain time limits for its reviews, permitted scrutiny of previously granted FCC licenses, and established formal authorities to request information from applicants.

Recent Actions by Team Telecom

- **Undersea Cable Network:** In June 2020, Team Telecom recommended that the FCC partially deny the Pacific Light Cable Network subsea cable system, to the extent it sought a direct connection between Hong Kong and the United States. Team Telecom separately granted portions of the project owned by Google and Facebook to connect Taiwan and the Philippines. Team Telecom noted "the PRC government's sustained efforts to acquire the sensitive personal data of millions of U.S. persons, the PRC government's access to other countries' data through both digital infrastructure investments and recent PRC intelligence and cybersecurity laws, and changes in the market that have transformed subsea cable infrastructure into increasingly data-rich environments that are vulnerable to exploitation."

- **Chinese Telecoms in the United States:** In April 2020, Team Telecom recommended the FCC revoke China Telecom (Americas) Corp.'s (a subsidiary of the PRC) authorization to provide telecommunications services in the United States. Per DOJ, in the recommendation U.S. agencies "identified substantial and unacceptable national security and law enforcement risks associated with China Telecom's operations."

- **China Mobile:** In May 2019, based on the recommendation of Team Telecom, the FCC denied China Mobile USA's application to provide telecommunications services in the United States. The order found that "due to … control by the Chinese government, grant of the application would raise substantial and serious national security and law enforcement risks that cannot be addressed through a mitigation agreement between China Mobile and the federal government."

CFIUS – Emerging Trends: China, China, China

- **Focus on Chinese Investments in Critical Technologies.** CFIUS scrutiny will continue, particularly with respect to Chinese investments in U.S. TID companies. In December 2020, U.S. Senators from both parties raised the alarm that Chinese state-backed funds seek to invest in U.S. critical technology companies, notwithstanding the reinvigorated CFIUS scrutiny.* We expect CFIUS to continue to examine Chinese involvement with third-country foreign acquirers.

- **New Bills.** In April 2021, two new bills were introduced to strengthen CFIUS's power in relation to China. The **Strategic Competition Act of 2021** was introduced to address multiple China-related issues, including expanding CFIUS jurisdiction to include deals or investments that involve institutions of higher education. The **Protecting Military Installations and Ranges Act of 2021** was introduced to direct CFIUS to investigate any acquisition of land near a military installation if the buyer has ties to China, Russia, Iran, or North Korea.

- **Whole-of-Government Pressure on China.** The Biden administration has continued its pressure on China. The Commerce Department has issued subpoenas to a number of Chinese companies in the information and communications technology and services ("ICTS") industry over national security concerns. During the Biden administration's first official meeting with China, Secretary of State Blinken raised his concerns with China's threat to "the rules-based order that maintains global stability."

* Mercedes Ruehl, James Kynge and Kiran Stacey, *Chinese State-backed Funds Invest in US Tech Despite Washington Curbs*, FIN. TIMES (Dec. 2, 2020).

DOJ's China Initiative

Launched in 2018, DOJ's China Initiative identified a series of goals and enforcement priorities related to countering threats posed by the Chinese government across a range of sectors:

- Prioritize investigations of economic espionage and trade secret theft
- Develop an enforcement strategy for non-traditional collectors, such as exploitation of universities and colleges
- Counter malicious cyber activity, such as the theft of personally identifiable information
- Counter malign foreign influence, including via FARA violations
- Counter foreign intelligence activities
- Conduct foreign investment reviews and bolster telecommunications security
- Conduct education and outreach

DOJ's China Initiative

The China Initiative has achieved significant success, but at the same time suffered from several prosecutorial setbacks and criticism that its focus on non-traditional collectors has unfairly targeted individuals of Chinese heritage. Even with these issues, the China Initiative—even if rebranded—is likely to continue in some form, given the range of threats posed by the Chinese government.

Notable China Initiative prosecution setbacks include:

- Anming Hu, an engineering professor at the University of Tennessee working on NASA projects, was indicted in February 2020 on charges of wire fraud and making false statements related to his alleged failure to disclose ties to a Chinese state-run university. The jury failed to reach a verdict and the judge declared a mistrial.

- In July 2021, DOJ dropped charges against Dr. Qing Wang, a researcher at the Cleveland Clinic, who was charged with wire fraud and false statements related to Chinese grant funding.

> "We will counter Chinese espionage and cyber and everything else but we won't forget the civil rights and civil liberties of the people in this country."
>
> - Attorney General Merrick Garland, June 2021

- Also in July 2021, DOJ dismissed its case against Dr. Juan Tang, a cancer researcher at University of California – Davis, for allegedly lying about previous service in the Chinese People's Liberation Army. Similar cases were dropped against Chinese researchers at other universities.

National Security Enforcement in the Biden Administration

- **Counterterrorism and Domestic Terrorism:** In May 2021, Attorney General Merrick Garland stated "Both forms of terrorism are of extraordinary concern to me. We never want to take our eyes off of what happened on 9/11 and the risks that our country continues to face from foreign-origin attacks on the homeland. Likewise, we have a growing fear of domestic violent extremism and domestic terrorism. Both of those keep me up at night." Accordingly, DOJ's focus on countering terrorist financing, particularly at the nexus of evolving technologies such as crypto-currency will almost certainly continue as a priority.

Image Source: Tom Brenner/POOL/EPA-EFE/Shutterstock

- **Continuing the China Initiative:** In statements, proposed legislation and administration priorities, President Biden has made clear that countering China will remain a priority, noting "We have to push back against the Chinese government's abuses and coercion that undercut the foundations of the international economic system. Everyone must play be the same rules." Even domestic policy priorities of the new administration, such as the "American Jobs Plan," note a goal to "unify and mobilize the country to meet the great challenges of our time: the climate crisis and the ambitions of an autocratic China." And at the G7 Summit in June 2021, President Biden stated, "China has to start to act more responsibly in terms of international norms on human rights and transparency."

Image Source: Mandel Ngan/Getty Images

National Security Enforcement in the Biden Administration

- **Continued Sanctions and Export Controls Enforcement:** Sanctions and export controls have been a "go-to" foreign policy and economic tool in recent administrations, a trend that is unlikely to change. The Biden Administration has already enacted new sanctions targeting **Russian** actors involved in political influence campaigns. The Biden administration is likely to leverage human rights-based sanctions, such as the Global Magnitsky Sanctions, to address abuses in **Burma** and as a means to pressure **China**. The new administration's stance on continuing President Trump's substantial sanctions on **Iran** will almost certainly be dependent on progress made in negotiations around Iran's nuclear program, where sanctions can be wielded as both carrot and stick.

- **Aggressive Prosecution of FARA Offenses:** Increased attention on foreign lobbying and influence efforts will likely continue to build momentum under the Biden administration, especially as it pertains to **Russia** and **Ukraine**. The scope of FARA investigations may broaden to include **Chinese** influence campaigns as well.

- **Foreign Investment:** The role and scope of CFIUS under the Biden administration is set to expand. Although the foreign actors of concern—largely **China**—will remain the same, CFIUS (as enabled by FIRRMA and potentially by proposed legislation) will increasingly focus on areas beyond CFIUS's traditional remit of industrial and real estate transactions. In particular, FIRRMA's expansion of CFIUS jurisdiction to cover certain classes of sensitive personal data and emerging technologies will likely comprise the new frontier of aggressive CFIUS review.

Zainab Ahmad

200 Park Avenue, New York
NY 10166-0193

Tel +1 212.351.2609
zahmad@gibsondunn.com

Zainab Ahmad is a partner in the New York office of Gibson, Dunn & Crutcher and a member of the firm's White Collar Defense and Investigations and Privacy, Cybersecurity and Consumer Protection Practice Groups. Ms. Ahmad served as Senior Assistant Special Counsel in Special Counsel Robert S. Mueller's Office following a successful career as a prosecutor and trial lawyer at the Department of Justice in both Washington, D.C., and the Eastern District of New York. As former Deputy Chief of the National Security and Cybercrime section at the U.S. Attorney's Office in the Eastern District of New York, Ms. Ahmad supervised a unit of over 20 attorneys, investigators, and staff prosecuting sensitive counterterrorism, counterespionage and cybercrime cases. Ms. Ahmad's practice focuses on white collar defense and investigations, as well as regulatory and civil litigation challenges, such as matters involving corruption, anti-money laundering, sanctions and FCPA issues. She also advises clients on cybercrime and intellectual property issues, including handling investigations, enforcement defense, and litigation. She has extensive experience with a wide range of federal, state, and international cybersecurity laws, regulations, and standards.

Prior to joining Gibson Dunn, Ms. Ahmad was a prosecutor with the U.S. Department of Justice for 11 years. She most recently served as a Senior Assistant Special Counsel in Special Counsel Robert S. Mueller's Office from 2017 to 2019. Prior, she served as an Assistant U.S. Attorney at the U.S. Attorney's Office in the Eastern District of New York, where her roles included Deputy Chief of the National Security and Cybercrime section. During her tenure, she prosecuted and supervised some of the most complex international terrorism investigations in the United States, focusing on al-Qaeda, ISIS and attacks against U.S. military personnel and U.S. diplomats abroad. In pursuit of these extraterritorial national security investigations, she worked closely with the FBI, U.S. intelligence community, Department of State and Department of Defense, and she frequently traveled to Europe, the Middle East and Africa to negotiate with foreign law enforcement officials and regulators for access to evidence and testimony, and to collaborate with foreign counterparts regarding mutual legal assistance requests and extradition assurances. Her work was chronicled in a The New Yorker feature article, "Taking Down Terrorists in Court."

During her career, Ms. Ahmad was seconded twice to Washington, D.C., serving in 2016 as Counselor for Transnational Organized Crime and International Affairs and in 2017 as Acting Deputy Assistant Attorney General in Washington, D.C., where she was responsible for supervising about 70 prosecutors in three sections: Organized Crime & Gangs, Human Rights and Special Prosecutions, and Capital Cases, including the filter team handling the "Panama Papers"-related investigations.

Drawing on her experience, Ms. Ahmad has played an active role in the advancement of global cybercrime laws and regulations. She previously represented DOJ at meetings of the World Economic Forum's Cybercrime Workshop and participated in development of WEF's Guidance on Public-Private Information Sharing Against Cybercrime. She also organized and led a Cybercrime Roundtable with former FBI Director James Comey and General Counsel and C-suite executives from various industries, including banking, media, health care and pharmaceutical companies, to discuss improved public-private partnership in combatting cybercrime.

Ms. Ahmad received her law degree in 2005 from the Columbia University School of Law, where she received the Hamilton Fellowship (full scholarship for academic excellence), was a James Kent Scholar and a Harlan Fiske Stone Scholar, and served as the Senior Editor of the Columbia Law Review. She served as a law clerk for Judge Jack B. Weinstein of the U.S. District Court for the Eastern District of New York from 2006 to 2007 and for Judge Reena Raggi of the U.S. Court of Appeals for the Second Circuit from 2007 to 2008.

David P. Burns

1050 Connecticut Avenue
N.W., Washington, DC 20036-5306

Tel +1 212.887.3786
dburns@gibsondunn.com

David P. Burns is a litigation partner in the Washington, D.C., office of Gibson, Dunn & Crutcher. His practice focuses on white-collar criminal defense, internal investigations, national security, and regulatory enforcement matters. Mr. Burns 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. He is the co-chair the firm's National Security Practice Group, and a member of the White Collar and Investigations and Crisis Management practice groups.

Prior to re-joining the firm, Mr. Burns 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, Mr. Burns 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.

Mr. Burns has been recognized by Chambers USA – America's Leading Business Lawyers as a leading White Collar attorney in the District of Columbia and Who's Who Legal and Global Investigations Review (GIR) recognized him as a leading investigations lawyer, deemed "excellent" for his work across "federal, state, and regulatory investigations." Who's Who Legal also recognized Mr. Burns as a leading lawyer in the area of Business Crime Defense.

Mr. Burns 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.

Robert K. Hur

1050 Connecticut Avenue
N.W., Washington, DC 20036-5306

Tel +1 202.887.3674
rhur@gibsondunn.com

Robert K. Hur is a partner in the Washington, D.C. office of Gibson, Dunn & Crutcher, and Co-Chair of the Firm's Crisis Management Practice Group. A seasoned trial lawyer and advocate, he brings decades of experience in government and in private practice, including service in senior leadership positions with the U.S. Department of Justice, to guide companies and individuals facing white-collar criminal matters, regulatory proceedings and enforcement actions, internal investigations, and related civil litigation. He is also a member of the firm's White Collar Defense and Investigations Practice Group and the National Security Practice Group.

Prior to joining Gibson Dunn, Mr. Hur served as the 48th United States Attorney for the District of Maryland. Presidentially appointed and unanimously confirmed by the United States Senate, he served from 2018 to 2021 as the chief federal law enforcement officer in Maryland, setting strategic priorities for and supervising one of the largest and busiest U.S. Attorney's Offices in the nation. During his tenure as United States Attorney, the Office handled numerous high-profile matters including those involving national security, cybercrime, public corruption, and financial fraud. In pursuit of sophisticated and impactful cases, Mr. Hur partnered closely with other enforcement agencies including the Securities and Exchange Commission, the Commodity Futures Trading Commission, the Department of Health and Human Services Office of Inspector General, and the Maryland Attorney General's Office. He also hired dozens of attorneys from diverse backgrounds to bring the Office to its maximum staffing level and as a member of the Attorney General's Advisory Committee, counseled the Attorney General on matters of policy, procedure, and management.

Before serving as United States Attorney, Mr. Hur served as the Principal Associate Deputy Attorney General with the Department of Justice in Washington, D.C. from 2017 to 2018. In the position of "PADAG," Mr. Hur was a member of the Department's senior leadership team and the principal counselor to Deputy Attorney General Rod J. Rosenstein, assisting him with oversight of all components of the Department including the National Security, Civil, Criminal, and Antitrust Divisions, all 93 U.S. Attorney's Offices, and the Federal Bureau of Investigation. He also liaised regularly on behalf of the Justice Department with the White House, Congressional committees, and federal intelligence, enforcement and regulatory agencies.

Mr. Hur is an accomplished trial lawyer, having tried fourteen cases as a federal prosecutor and in private practice. He was a member of the trial team that won a clean-sweep acquittal in 2016 for Vascular Solutions, Inc., a publicly traded medical device company, in a groundbreaking federal criminal trial involving off-label promotion charges. More recently, in 2020 as United States Attorney, he tried and won conviction in an international money-laundering trial that was the first in-person federal jury trial conducted in the Washington, D.C. region during the COVID-19 pandemic.

Mr. Hur serves as Chair of the Asian American Hate Crimes Workgroup, a statewide body formed by Governor Larry Hogan and charged with developing strategies, recommendations, and actions to address the rise in violence and discrimination targeting the Asian American community. He is an active member of the Alliance for Asian American Justice, a national pro bono initiative providing legal services to victims of anti-Asian hate, and previously served on the Board of Directors of the Asian Pacific American Bar Association of the District of Columbia (APABA-DC).

Adam M. Smith

1050 Connecticut Avenue
N.W., Washington, DC 20036-5306

Tel +1 202.887.3547
asmith@gibsondunn.com

Adam M. Smith is a partner in the Washington, D.C. office of Gibson, Dunn & Crutcher. He is an experienced international lawyer with a focus on international trade compliance and white collar investigations, including with respect to federal and state economic sanctions enforcement, CFIUS, the Foreign Corrupt Practices Act, embargoes, and export controls. In 2019, 2020, and 2021 Mr. Smith was ranked nationally by *Chambers USA* as a leading attorney in International Trade: Export Controls & Economic Sanctions. Mr. Smith was also identified by *Global Investigations Review* as one of the leading sanctions practitioners in Washington, DC.

From 2010-2015 Mr. Smith served in the Obama Administration as the Senior Advisor to the Director of the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) and as the Director for Multilateral Affairs on the National Security Council. At OFAC he played a primary role in all aspects of the agency's work, including briefing Congressional and private sector leadership on sanctions matters, shaping new Executive Orders, regulations, and policy guidance for both strengthening sanctions (Russia and Syria) and easing measures (Burma and Cuba), and advising on enforcement actions following sanctions violations.

Mr. Smith traveled extensively in Europe, the Middle East, Asia, Africa, and the Americas conducting outreach with governments and private sector actors on sanctions, risk, and compliance. This outreach included meetings with senior leadership in several sectors including finance, logistics, insurance and reinsurance, energy, mining, technology, and private equity.

Mr. Smith frequently chaired the Treasury delegation to EU/G7 consultations regarding Russia sanctions and negotiated with EU institutions and member states to implement coordinated measures. Additionally, Mr. Smith managed the development and implementation of the U.S. government's international outreach program on Congressionally-mandated Iran sanctions and helped develop proposed sanctions relief strategies as a part of the Iranian nuclear negotiations.

During Mr. Smith's tenure on the White House's National Security Council he advised the President on his multilateral agenda including with respect to international sanctions, coordinated inter-agency efforts to relieve U.S. economic restrictions on Burma, and developed strategies to counter corruption and illicit flows and to promote stolen asset recovery.

Mr. Smith's expertise is sought out by governments, academia, and other law firms; he has served as an expert witness in several international arbitration matters, and his analysis can be frequently seen in print and broadcast media (including in *The Economist*, the *Wall Street Journal*, the *N.Y. Times*, and the *Washington Post*, and on BBC and NPR). He is the author of three legal texts and dozens of articles and book chapters, has testified before the U.S. Congress, and is a frequent presenter at industry, governmental, and academic conferences globally. Earlier in his career, Adam was a political economist at the United Nations and also held posts at the World Bank and the OECD.

Courtney M. Brown

1050 Connecticut Avenue
N.W., Washington, DC 20036-5306

Tel +1 202.887.3502
cmbrown@gibsondunn.com

Courtney M. Brown is a senior associate in the Washington, D.C. office of Gibson, Dunn & Crutcher, where she practices primarily in the areas of white collar criminal defense and corporate compliance. Ms. Brown has experience representing and advising multinational corporate clients and boards of directors in internal and government investigations on a wide range of topics, including anti-corruption, anti-money laundering, sanctions, securities, tax, and "me too" matters.

Selected investigation and enforcement matters include:

- Represented a multinational information technology company in negotiating resolutions of claims brought by the U.S. Department of Justice ("DOJ") and Securities and Exchange Commission ("SEC") under the U.S. Foreign Corrupt Practices Act ("FCPA"), including successful completion of a post-resolution reporting period.
- Conducted an investigation for the Board of Directors involving allegations of insider dealing against executives.
- Represented a global financial institution in a multi-agency investigation concerning the U.S. Treasuries market.
- Conducted a workplace investigation on behalf of a Special Committee of the Board of Directors.
- Represented an investment manager in an SEC investigation involving allegations of false advertising and other misconduct under securities regulations.
- Represented a defense company, obtaining declinations of criminal and civil enforcement actions by the DOJ and SEC in FCPA investigations, as well as the dismissal of an employment lawsuit brought by a former employee.
- Obtained declinations, on behalf of a Fortune 500 company, of criminal and civil enforcement actions by the DOJ and SEC in a joint FCPA investigation arising from whistleblower complaints.
- Represented banks and asset managers in investigations by the DOJ, SEC, congressional committees, and state investigators relating to subprime mortgage matters and the Madoff fraud.

Ms. Brown 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, anti-money laundering regulations, and economic and trade sanctions administered by the U.S. Department of Treasury's Office of Foreign Assets Control.

Ms. Brown has participated in two government-mandated FCPA compliance monitorships and conducted anti-corruption and compliance trainings for in-house counsel and employees. She also has experience advising companies on the application of the U.S. Sentencing Guidelines and, since 2014, has been a contributing author for the ABA's treatise, "Practice Under the Federal Sentencing Guidelines."

Ms. Brown completed a secondment at a Fortune 100 company, where she advised global legal and business teams on compliance with anti-corruption laws.