Department of Justice

STATEMENT OF
NICOLE ARGENTIERI
ACTING ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

&

MATTHEW OLSEN
ASSISTANT ATTORNEY GENERAL
NATIONAL SECURITY DIVISION

BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED
"CLEANING UP THE C-SUITE: ENSURING ACCOUNTABILITY FOR CORPORATE CRIMINALS"

PRESENTED
DECEMBER 12, 2023

INTRODUCTION

The Department has long prioritized white collar and corporate criminal enforcement to ensure that both corporate and individual white-collar offenders are held accountable. As Attorney General Merrick Garland said, "there is not one set of laws for the powerful and another for the powerless; one for the rich and one for the poor." By demanding accountability in our white collar and corporate prosecutions, we are reaffirming our commitment to the rule of the law and to protecting the American people.

Today's dynamic threat landscape demands that the Department of Justice expand, innovate, and modernize our white collar and corporate enforcement efforts to meet the moment. As Deputy Attorney General Lisa Monaco said, "Corporate enforcement is in an era of expansion and innovation."

To meet the moment, the Department is modernizing, adapting, and devoting substantial resources to our fight against white collar and corporate crime and has made significant innovations in our enforcement efforts. Since 2021, the Department has announced policy updates intended to protect the public, promote the integrity of our markets, discourage unlawful business practices, fight transnational corruption, ensure confidence in our economic system, and uphold the rule of law.

Concurrent with the policy announcements in an October 28, 2021, Memorandum ("2021 Memorandum") issued by the Deputy Attorney General, the Department established the Corporate Crime Advisory Group (CCAG) to review the Department's corporate enforcement policies. The resulting updated policies ensure individual accountability, discourage corporate recidivism, promote strong corporate culture, encourage cooperation and compliance, enable detection of wrongdoing with voluntary self-disclosure, and reinforce public confidence in the evenhanded administration of justice and the fairness of our system. Underlying all of these policies—and our corporate enforcement generally—is the Department's commitment to appropriate transparency and to building public confidence in our work.

Through the same 2021 Memorandum, the Department announced several policies designed to incentivize increased corporate compliance and to ensure effective deterrence. The Department directed prosecutors to take a holistic approach to assessing a corporation's past misconduct—considering all misconduct that was the subject of any prior domestic or foreign criminal, civil, or regulatory enforcement actions against the corporation—in determining whether the company lacks appropriate internal controls or corporate culture that disincentivizes criminal activity. The Department also revised guidance regarding corporate monitors, directing Department attorneys to carefully assess, in each case, whether there is a demonstrated need for, and clear benefit to be derived from, a monitorship, such as where internal controls are untested, ineffective, inadequately resourced, or not fully implemented.

In addition, the 2021 Memorandum reinstated prior guidance that to qualify for any cooperation credit, corporations must provide to the Department all relevant facts relating to the individuals responsible for the misconduct, regardless of their position, status, or seniority, and provide to the Department all nonprivileged information relating to that misconduct. Following

the CCAG's review, in 2022, the Department took further significant steps to prioritize individual accountability. At the direction of the Deputy Attorney General, every Department component that did not already have a voluntary self-disclosure policy has now adopted one. For the first time, all 94 U.S. Attorney's Offices have now adopted a single voluntary self-disclosure policy. The goal of these policies is to identify misconduct at the earliest possible opportunity. That way, we can put a stop to the conduct and take swift and effective action against individual wrongdoers—enhancing the individual accountability that is our top priority in fighting white collar crime. Corporations seeking cooperation credit not only must disclose all relevant, nonprivileged facts about individual misconduct, but also disclose *without delay*—such that prosecutors have the opportunity to effectively investigate and seek criminal charges against culpable individuals. The criteria and predictable results of voluntary self-disclosure are laid out in black and white in component policies that are publicly available on the Department's website. Improved corporate compliance safeguards the public, increases the fairness and reliability of markets, and protects our collective security.

The Department has also directed prosecutors to prioritize individual accountability by striving to complete investigations into individuals—and seek any appropriate and factually and legally supported individual criminal charges—prior to or simultaneously with the entry of a resolution against the corporation. This approach is resource-intensive: prosecuting the most sophisticated and far-reaching cases requires breaking down complex criminal schemes, understanding cutting-edge markets, and analyzing terabytes or even petabytes of data, with high-powered defendants mounting aggressive defenses and hiring sophisticated counsel.

In addition to our focus on deterrence and accountability for traditional forms of corporate crime, the Department's corporate enforcement efforts are evolving to address the rapidly increasing intersection between corporate crime and the risks that threaten U.S. national security. From terrorist financing, sanctions evasion, and export control circumvention to cyber- and crypto-enabled crime, sophisticated white collar criminals are threatening U.S. national security. As the threats have changed, so too has the Department's approach. In addition to remaining committed to existing efforts, such as the fight against foreign bribery, we are investing resources into new fields, including cybercrime and cryptocurrency, and surging resources to sanctions evasion and export controls.

Our whole-of-Department approach to combating corporate crime is reflected by the focused work of multiple Department components on these priorities. The recent announcement of the resolution in the Binance matter epitomizes this holistic approach at the intersection of corporate criminal and national security challenges. Just three weeks ago, the Department announced its largest corporate resolution that also involved the guilty plea of a chief executive officer (CEO). Binance pleaded guilty to violating the Bank Secrecy Act, failing to register as a money transmitting business, and violating U.S. sanctions, and Binance's CEO, Changpeng Zhao, pleaded guilty to causing Binance to violate the Bank Secrecy Act. Binance agreed to pay $4.3 billion in penalties, to the imposition of an independent monitor, and to enhance its compliance program. These historic guilty pleas were the result of collaboration between the Criminal Division and the National Security Division (NSD), coupled with critical partnership from the U.S. Attorney's Office for the Western District of Washington. This case is just the latest example of the Department's commitment to investigate and prosecute the most complex,

impactful corporate criminal schemes across a wide range of industries.

But this work to investigate and prosecute the most complex corporate crime, including crime that threatens national security, also presents challenges. Major investigations require major investments in time, money, and personnel. Our ability to collect a growing array of electronic evidence is limited by our capacity to process, store, and review that evidence. And well-resourced white collar and corporate defendants are using every tool available in an attempt to escape accountability, especially as we insist on guilty pleas for corporations and pursue stiff jail sentences for individuals where appropriate.

Underlying all of these policies—and our corporate enforcement generally—is the Department's commitment to appropriate transparency and to building public confidence in our work. Clear expectations for corporations are an integral part of ensuring appropriate compliance.

CRIMINAL DIVISION

I. Mission and Scope of Work

The Criminal Division's mission is to serve the public interest through the enforcement of criminal statutes vigorously, fairly, and effectively. White collar and corporate crime enforcement is a top Criminal Division priority. Many of the Criminal Division's sections are involved in this important work, including the Fraud Section, which prosecutes all violations of the Foreign Corrupt Practices Act (FCPA) as well as securities and commodities fraud, consumer fraud, procurement fraud, and health care fraud; the Money Laundering and Asset Recovery Section (MLARS), which prosecutes financial institutions and their employees for violations of the Bank Secrecy Act, sanctions, money laundering and related offenses, and third party money launderers and kleptocrats; and the Computer Crime and Intellectual Property Section (CCIPS), which prosecutes cybercrime in its many forms, trade secret theft and other intellectual property offenses, and the growing number of crimes involving cryptocurrency. The Criminal Division's sections often work together—as well as with U.S. Attorney's Offices around the country and in coordination with international partners—to bring the worst corporate offenders to justice.

Corporate crime results from individual wrongdoers who engage in misconduct and faulty institutional structures that those individuals often exploit. That is why effective enforcement in this area includes prosecution of both individuals and organizations. Our number one priority in this area is individual accountability, but this does not come at the expense of corporate responsibility. Corporate malfeasance—including bribery, market manipulation, anti-money laundering violations, and sanctions evasion—harms individuals, organizations, and governments, including our democratic institutions by undermining public trust in the rule of law. The Criminal Division aggressively prosecutes such crimes and brings perpetrators to justice. The fight against corporate crime requires substantial resources, innovative thinking, and increasingly international cooperation in our enforcement efforts, as the Criminal Division goes after offenders who perpetrate and try to conceal their crimes in increasingly sophisticated ways.

II. The Criminal Division's Enforcement Priorities

Despite the COVID-19 pandemic and the resulting case backlog, we broke records over the past two years by securing the highest number of individual fraud convictions and obtaining groundbreaking convictions against senior executives. Individual accountability is critical to effective enforcement in this space. It deters misconduct by putting potential wrongdoers on notice that they cannot hide behind the corporate form, and it incentivizes positive changes in corporate behavior. Holding individuals accountable for their illegal wrongdoing—including in the corporate context—also reinforces public confidence in the evenhanded administration of justice and the fairness of our system.

Ensuring justice for victims of crimes is also central to maintaining public confidence in our work—and therefore is at the forefront of that work. The Department renewed this commitment through the Attorney General's Guidelines for Victim and Witness Assistance (Guidelines), which the Department revised last year. The revised Guidelines prioritize a victim-centered, trauma-informed, and culturally sensitive approach to prosecutions and emphasize that treating victims with dignity and respect is essential to the Department's mission. The Guidelines encourage Department personnel to go beyond our legal obligations to provide assistance to other persons and entities who are significantly harmed by criminal conduct, but who may not fall within the statutory definition of a crime victim. To help implement these Guidelines, the Criminal Division and all U.S. Attorney's Offices have designated prosecutors to serve as victim-witness coordinators, and the Criminal Division has also designated a Victim Policy Coordinator who sits in the Office of the Assistant Attorney General. Having dedicated prosecutors with relevant expertise and experience serve as a resource for other Department personnel helps ensure that victims' rights remain a priority at all levels. We are committed to empowering and vindicating victims and ensuring they are afforded their rights through the criminal justice process.

A. The Fraud Section

The Fraud Section investigates and prosecutes complex white collar crime throughout the country. The Fraud Section brings impactful, complex corporate and individual cases against those who perpetrate sophisticated criminal fraud schemes. The Fraud Section's FCPA Unit has unique responsibility for prosecuting violations of the FCPA by individuals and companies, and in doing so, is expanding and deepening its international partnerships around the world, including, among others, with the United Kingdom, Brazil, Malaysia, Switzerland, Ecuador, France, South Africa, Colombia, the Netherlands, and Singapore. For example, in a series of cases against companies that trade oil and other commodities, we have secured one corporate guilty plea as well as one deferred prosecution agreement for widespread bribery and other offenses. These cases have resulted in over $800 million in total criminal penalties and disgorgement. As part of our investigations into trading companies, we have charged 13 individuals. Through these cases, we have worked in coordination with multiple international partners, which has made evidence easier to obtain, led to criminals having fewer places to hide, and helped us recover criminal proceeds wherever they may be found.

The Fraud Section has set records in our prosecution of culpable individuals. In 2022, the

Fraud Section had a record number of trials—51. And in 2021 and 2022, we secured more individual fraud convictions than we had in any of the preceding six years. This year, we have set a record high in the average alleged loss amount per defendant charged by the Fraud Section—over $25 million. As these statistics demonstrate, we are focused on the worst of the worst offenders and achieve groundbreaking convictions against several senior executives in high-profile and complex matters. For instance, in 2020, in the Eastern District of New York, Goldman Sachs agreed to pay a total of over $2.9 billion for its participation in a scheme to pay over $1 billion in bribes to Malaysian and Abu Dhabi officials to obtain lucrative business, including by underwriting approximately $6.5 billion in three bond deals for 1Malaysia Development Bhd (1MDB). In addition to the FCPA corporate resolution, the Fraud Section and MLARS, together with our partners in the U.S. Attorney's Office for the Eastern District of New York, successfully prosecuted two high-ranking Goldman Sachs executives, including Roger Ng, a former Managing Director, who was convicted after trial in 2022 and sentenced to 10 years' imprisonment.

We have also convicted executives at trial for perpetrating fraud schemes. As one example, in April 2023, three former executives of Outcome Health, a Chicago-based health technology start-up company, were convicted after trial for their roles in a scheme that targeted the company's clients, lenders, and investors and involved approximately $1 billion in fraudulently obtained funds. In October 2023, Mark Schena, the president of a Silicon Valley-based medical technology company, was sentenced to eight years in prison, after his conviction at trial, and ordered to pay $24 million in restitution for participating in a scheme to defraud investors and a scheme to commit health care fraud and pay illegal kickbacks in connection with the submission of over $77 million in claims for COVID-19 and allergy testing.

The Fraud Section is innovative in its use of data to detect, investigate, and prosecute crimes. The Section has long proactively used data to combat the most egregious frauds on the Medicare and Medicaid programs. In addition, by assessing trading data and publicly available information, the Fraud Section's Market Integrity and Major Frauds Unit has identified company insiders who greatly outperformed the market when trading pursuant to 10b5-1 plans, which allow corporate insiders who are not in possession of material, non-public information to set up pre-planned stock transactions. This proactive analysis and our subsequent investigation led to the arrest of Terren Peizer, the founder and former CEO of Ontrak, a behavioral-health-services company, for insider trading—the Department's first ever insider-trading charges based exclusively on activity conducted pursuant to a 10b5-1 plan.

B. The Money Laundering and Asset Recovery Section

MLARS investigates and prosecutes complex international and domestic white collar cases involving financial institutions, kleptocrats, money laundering, and asset forfeiture. MLARS leads the Department's asset forfeiture and anti-money laundering enforcement efforts. It also manages the Department's asset forfeiture program, including distributing forfeited funds to victims of crime. The Section also initiates, coordinates, and reviews legislative and policy proposals that affect the asset forfeiture program and the Department's money laundering enforcement authorities.

MLARS's Bank Integrity Unit (BIU) focuses on corporate criminal schemes, investigating and prosecuting financial institutions and their insiders when their actions threaten the institution itself or the broader financial system. With roughly a dozen prosecutors, since its founding in 2010, the BIU has imposed more than $24 billion in financial penalties in criminal resolutions with global financial institutions that engaged in anti-money laundering, money laundering, sanctions, and other violations—including over $16 billion in penalties in its longstanding effort to hold financial institutions accountable for sanctions violations. To strengthen these efforts, earlier this year, we announced a surge of resources to the BIU, which will add six prosecutors to target economic sanctions-related financial misconduct.

MLARS is also a key contributor to priority Department initiatives targeting white collar crime, including Task Force KleptoCapture and the National Cryptocurrency Enforcement Team (NCET). MLARS participates in Task Force KleptoCapture in partnership with the NSD, and is focused on bringing forfeiture and money laundering expertise to investigations and prosecutions of those who seek to evade U.S. sanctions related to Russian aggression in Ukraine. In support of these efforts, MLARS, working with NSD and U.S. Attorney's Offices, has seized assets and charged corporate executives. For example, MLARS recently brough civil forfeiture proceedings against a $300 million luxury yacht owned by a sanctioned Russian oligarch, and obtained as seizure warrants for two jets associated with oligarchs and their entities. MLARS investigated and prosecuted the president of Florida steelmaking company Metalhouse and his co-conspirator, resulting in guilty pleas to money laundering conspiracy for transferring over $150 million to a sanctioned oligarch. These defendants prioritized their profits over compliance with U.S. sanctions and paid the price—pleading guilty to federal criminal charges.

C. The Computer Crime and Intellectual Property Section

CCIPS is responsible for implementing the Department's national strategies in combating computer and intellectual property crimes worldwide. CCIPS is the largest office in the Department prosecuting cybercrime, with over 45 permanent attorneys, handling more than 200 prosecutions or other criminal matters each year. Within the Department, CCIPS maintains primary responsibility for developing the Department's overall computer and intellectual property offense enforcement strategies, and for coordinating computer crime and intellectual property investigations and cases that may significantly impact more than one district or other countries.

In January, we announced that Federal Bureau of Investigation agents, with the support of CCIPS prosecutors, had infiltrated the Hive ransomware network's computers, disrupting the Hive group's attempts to extort victims around the world. Beginning in 2021 and operating largely from overseas, the Hive ransomware group attacked over 1,500 victims in more than 80 countries, including hospitals and other critical infrastructure victims in the United States. The Department's Hive team obtained covert access to the Hive networked, obtained the decryption keys necessary to access the victim's inaccessible data, and distributed them to over a thousand victims, allowing those victims to decrypt and thus regain access to their data. For example, the FBI disrupted a Hive ransomware attack against a Texas school district's computer systems. The Bureau provided decryption keys to the school district, saving it from making a $5 million ransom payment. That same month, the FBI disrupted a Hive ransomware attack on a

Louisiana hospital, saving the victim from a $3 million ransom payment. Critically, the team was able to provide over 300 Hive victims with decryption keys before they paid any ransom, thus thwarting ransom demands of over $130 million. As a final blow against Hive, the team and its international partners identified the main computers powering Hive ransomware and effectively dismantled Hive as a threat. The Hive dismantlement embodies the Department's strategy of using technical disruptions and all available tools to combat cybercrime, and the Department's prioritization of victims of cybercrime.

And earlier this year, the NCET became a part of CCIPS. The NCET will continue its leadership role in the Department's efforts to investigate, prosecute, and disrupt criminal activity involving cryptocurrency. In less than two years, the NCET has already been incredibly successful in its efforts to address the criminal misuse of cryptocurrencies and digital assets through large-scale enforcement actions.

D. Partnerships with U.S. Attorney's Offices

The Criminal Division partners with U.S. Attorney's Offices across the country to carry out the Department's mission. The Fraud Section, MLARS, and CCIPS investigate and prosecute complex white collar and corporate cases that often span multiple federal districts, and Criminal Division personnel work closely with Assistant U.S. Attorneys around the country in pursuit of the Department's corporate enforcement priorities. These partnerships can take the form of jointly prosecuting cases, as reflected in some of the examples highlighted above. In addition, Criminal Division sections regularly share their subject matter expertise with U.S. Attorney's Office counterparts.

In addition to joint cases with the Criminal Division, the U.S. Attorney's Offices also prosecuted cases focusing on individual accountability for corporate officers, such as the recent trial of former FTX CEO Sam Bankman-Fried and the prosecution of Allianz Global Investors U.S., its Chief Investment Officer, and two others—both cases in the Southern District of New York; and the trials of Theranos founder Elizabeth Holmes and former chief operating officer Ramesh "Sunny" Balwani in the Northern District of California.

III. The Criminal Division Approach to Corporate Criminal Enforcement

Voluntary self-disclosure of misconduct and cooperation by companies allow us to build stronger cases against culpable individuals more quickly. As searching as our investigations may be, there is some misconduct that we may never learn about absent a company's voluntary self-disclosure. To encourage cooperation and voluntary self-disclosure, the Department will not seek a guilty plea where a corporation has timely and voluntarily self-disclosed wrongdoing, fully cooperated in the investigation, and appropriately remediated the conduct. In 2023, the Department extended to the mergers and acquisition context the benefits of increased detection, deterrence, and compliance from voluntary self-disclosure by providing that a company can receive a presumption of a declination for misconduct it voluntarily self-discloses within six months from the date of closing, with a one-year timeline for remediation. This policy does not impact civil merger enforcement, nor does it apply to information that already was required to be disclosed. By having companies come forward, we will prevent crimes from going undetected,

and we will be better able to hold individual corporate wrongdoers accountable.

In addition to Department-wide policies, the Criminal Division has implemented additional policies specifically targeted to corporate crime. Our goal is to encourage companies to build strong compliance programs, work to detect and disclose wrongdoing, cooperate with the Department, and remediate any misconduct. This allows us to hold corporations to account and to prosecute culpable individuals, which remains our number one priority in this area.

In January 2023, the Criminal Division announced the first substantive changes in five years to the Corporate Enforcement and Voluntary Self-Disclosure Policy (CEP). Under the revised policy, there are greater incentives for companies that voluntarily self-disclose wrongdoing to the Criminal Division, including potential declinations with disgorgement and greater potential fine reductions where a criminal resolution is warranted. Companies that do not voluntarily self-disclose misconduct but fully cooperate and remediate the misconduct are eligible for reduced financial penalties. The revised CEP also makes clear that we will use varying starting points within the applicable Sentencing Guidelines range in order to fairly and meaningfully distinguish between companies. The new policy also expands and clearly spells out the circumstances in which companies can expect the Criminal Division to issue a CEP declination so long as the company disgorges any ill-gotten profits and pays any required restitution.

Further, in March of this year, the Criminal Division announced its three-year Compensation Incentives and Clawbacks Pilot Program. The Criminal Division believes that companies should include compliance-related criteria in their compensation and bonus systems, in order to create appropriate incentives for executives and other employees. Compensation systems that use affirmative metrics and benchmarks can reward compliance-promoting behavior. Compensation systems that clearly and effectively impose financial penalties for misconduct can also deter risky behavior and foster a culture of compliance. We also want to encourage companies to claw back or withhold compensation from culpable executives, which will shift the burden of financial penalties resulting from criminal conduct onto individual wrongdoers and away from often innocent shareholders. Under the Pilot Program, every corporate resolution now includes a requirement that the resolving company develop compliance-promoting criteria within its compensation and bonus system, subject to local labor laws. The Criminal Division then provides fine reductions to companies that seek to recoup compensation from corporate wrongdoers.

IV. Challenges

These accomplishments have been achieved notwithstanding the unique challenges that corporate criminal investigations and prosecutions present. Bigger, more complex cases require more resources—prosecutors, agents and analysts, data processing, and other IT capabilities. More defendants are taking their cases to trial, which requires the devotion of even more significant prosecutorial resources. Increasingly global investigations require investing time and resources into building partnerships with foreign law enforcement authorities—partnerships that can yield dividends both at home and abroad—and navigating the intricacies and challenges of obtaining evidence overseas, such as mutual legal assistance requests, data privacy rules, and

blocking statutes.

We need resources—including data analysts and data analytic tools—to exploit data to identify and disrupt criminal activity. The Fraud Section's exciting data analytics programs are being run on a relatively modest annual budget of $400,000. These complex cases involve voluminous, usually electronic, evidence and require substantial investment of personnel and time to review materials, but the systems we have in place to help with the organization and review of this evidence are not cutting edge. If we were to invest more, we could much more quickly build a technological framework to identify market manipulation and generate additional leads for FCPA cases. Such investments will pay dividends in our ability to go after even more corporate crime in the future.

In addition, while we are bringing important and complex prosecutions using the legislative tools available, with more tools we can do more. We have proposed a number of legislative fixes that would address some of the gaps in our enforcement authorities, including to address the sophisticated enforcement environment in an ever-increasingly digital world. In particular, we are focused on additional legislative tools that will expand our ability to prosecute criminal activity involving digital assets. These include adapting current laws to extend statutes of limitations for certain complex crimes including offenses involving digital assets and cybercrime, to increase the statutory maximum sentences for operating a cryptocurrency exchange or other money transmitting businesses without registering, and to expand the predicate crimes for money laundering offenses. The Department looks forward to working with Congress on these and other needed statutory changes.

NATIONAL SECURITY DIVISION

I. The Evolving National Security Landscape

The National Security Division (NSD) is charged with carrying out one of the Department of Justice's highest priorities: to defend the national security of the United States by pursuing justice under the law, including by investigating and prosecuting terrorism, espionage, sanctions and export violations, foreign malign influence, and malicious cyber activity; overseeing and supporting the Intelligence Community's lawful use of surveillance authorities to acquire intelligence; and reviewing the national security risks of proposed foreign investments in U.S. companies. NSD regularly contributes to the whole-of-government response to the most serious threats we face as a nation.

Today, the United States faces dynamic threats from a range of highly capable nation-state actors, including China, Russia, Iran, and North Korea. These nations engage in aggressive and sophisticated efforts, both inside our borders and abroad, to undermine the security, economic interests, and democratic institutions of the United States and our allies.

Nation-state adversaries seek to evade U.S. sanctions and export controls to develop capabilities that threaten international peace and stability. These countries seek to obtain critical emerging technologies, including military hardware, cutting-edge semiconductors, and advanced computing capabilities. These technologies pose significant dangers in the hands of our

adversaries, with the potential to undermine advantages in U.S. and allied military capabilities. But the harms are not limited to military applications. Repressive regimes can use dual-use technologies like artificial intelligence, facial recognition, and advanced biotechnologies to conduct surveillance of civilian populations, stifle dissent, and enable human rights abuses.

Hostile nations are also accelerating their use of cyber-enabled means to carry out a range of activity targeting the U.S. government and American businesses and households. This includes stealing sensitive technologies, trade secrets, intellectual property, and sensitive personal data, as well as seeking access to hold our critical infrastructure networks at risk for destructive or disruptive attacks. While an increasing number of adversary nations conduct malicious activity in cyberspace, the People's Republic of China continues to stand apart in the breadth of persistent threats it poses to U.S. government and private-sector networks, including U.S. critical infrastructure.

In responding to this threat landscape, in which national security and corporate responsibility intersect, the National Security Division increasingly is focused on the role of the private sector and corporate enforcement. When it comes to corporate responsibility, NSD seeks to incentivize corporations to invest in well-functioning compliance programs with a focus on their obligations to national security.

II. The National Security Division's Enforcement Priorities

The mission and the changing threat landscape drive the National Security Division's enforcement priorities. As NSD's enforcement priorities respond to confront evolving threats, our efforts increasingly interact with corporations and the business community.

The continued challenge posed by terrorism, and the rising challenge posed by nation-state adversaries to the United States has placed even greater emphasis on the enforcement of the laws we use to defend against such threats. Those enforcement areas—sanctions, export controls, cyber, economic espionage, countering foreign malign influence, and foreign investment review—have gained increased salience in the fight to secure America's future against nation-state threat actors.

Across these priorities, NSD's relationship with the private sector is multi-faceted. Where firms are witnesses to or victims of threats to our national security, the private sector plays a vital and cooperative role in helping to defend our nation. Responsible financial institutions stand as gatekeepers to the global financial system, shutting out sanctioned parties and monitoring for and reporting suspicious activity. And our critical infrastructure industries, and the firms whose innovations help maintain our nation's competitive advantage, are key partners in protecting our country against cyber threats. But when these companies place our nation's security at risk by violating our national security laws, NSD does not and will not hesitate to investigate and prosecute them. Where firms choose to make business decisions to undermine our nation's security by committing crimes for their own profit, we will seek to hold these firms accountable.

A. Terrorism

Combating terrorism, both international and domestic, remains core to the mission of the National Security Division. And we have seen recent instances in which our counterterrorism work intersects with our increasing focus on corporate responsibility. Most notably, last fall, NSD's Counterterrorism Section, working with the U.S. Attorney's Office for the Eastern District of New York, secured the Department's first-ever corporate guilty plea to a charge that a company conspired to provide material support and resources to a foreign terrorist organization. That case, against Lafarge SA, a multinational cement company based in France, held the company accountable for the actions of its executives, who paid the equivalent of millions of dollars to ISIS to increase profits and market share in Syria—all while ISIS engaged in a campaign of violence during the Syrian civil war. The company paid fines and forfeiture of approximately $778 million, while the French government has prosecuted the individual French executives. The Lafarge prosecution sent a clear message that NSD will not hesitate to hold corporations responsible if they make payments to designated terrorist organizations in furtherance of market share and profits.

B. Sanctions

Economic sanctions are a critical national security tool that seek to impose consequences on our adversaries and change their behavior by denying them access to the U.S. market and the economic benefits that come from doing business with the United States. Most economic sanctions programs are imposed by the President under the International Emergency Economic Powers Act (IEEPA) and administered by the Department of the Treasury's Office of Foreign Assets Control, and can be either comprehensive or selective, using the blocking of assets and trade restrictions to target countries and groups of individuals, including longstanding sanctions programs targeting Iran, Russia, and North Korea. NSD prosecutes criminal violations of IEEPA and other crimes related to the violation or evasion of U.S. sanctions, such as money laundering.

Large multi-national corporations, financial institutions, and defense contractors (among others) bear responsibility for ensuring they have a well-functioning compliance program and are adhering to U.S. sanctions—and NSD's criminal actions underscore the costs of failing to meet this obligation. For example, NSD, together with the U.S. Attorney's Office in Washington D.C., announced earlier this year a record-breaking resolution with British American Tobacco (BAT), one of the world's largest manufacturers of tobacco products, and its subsidiary, BAT Marketing Singapore (BATMS). BAT, through a third-party company, did business in North Korea resulting in approximately $418 million of banking transactions, generating revenue used to advance North Korea's weapons program. In April 2023, BATMS pleaded guilty to, and BAT entered into a deferred prosecution agreement to resolve, charges that they conspired to commit bank fraud and violate IEEPA, paying penalties totaling more than $629 million to resolve these charges, making it the largest-ever criminal penalty imposed in connection with a violation of the sanctions program against North Korea.

Since Russia's unprovoked invasion of Ukraine, the Department has placed significant additional resources and emphasis on investigating violations of U.S. sanctions targeting Russian oligarchs, proxies, and other regime supporters. Much of this work has taken place under Task

Force KleptoCapture, in which NSD and the Criminal Division play central roles. The Department's key enforcement actions have included October 2022 charges of nearly a dozen individuals and several corporate entities with participating in unlawful sanctions evasion and money laundering schemes to export powerful, civil-military, dual-use technologies to Russia and ship them to Russian end users, including sanctioned companies that serviced Russia's military.

Some of the central features of these technologies—including the ability to conduct nearly anonymous and instantaneous cross-border transactions—can pose significant risks to the public and to national security by facilitating crimes of all sorts, including sanctions evasion, terrorist financing, ransomware targeting critical infrastructure, and money laundering.

C. **Export Controls**

Export controls are a critical tool to prevent our adversaries from eroding the technological advantage created by U.S. innovation and economic growth. The Commerce Department's Bureau of Industry and Security (BIS) and the State Department's Directorate of Defense Trade Controls (DDTC) are primarily responsible for regulating the export of items, services, and technologies to other countries and foreign nationals, under the Export Control Reform Act and the Arms Export Control Act. BIS and DDTC use these authorities to prevent the export of sensitive items and technologies to our adversaries. The National Security Division is responsible for the criminal prosecution of those who willfully violate these export controls.

Our adversaries are determined to unlawfully acquire advanced and sensitive technology from the United States and from our allies. For example, Russia is trying to circumvent heightened controls imposed on component parts being used in weapons systems against Ukraine. Because Russia needs this equipment to support its war effort and cannot manufacture enough of it domestically, it has turned to using third-party intermediaries and transshipment points to disguise the transfer of prohibited items and to hide the fact that the items are destined for Russian end users.

In February 2023, the National Security Division joined with the Commerce Department's BIS to set up the Disruptive Technology Strike Force, an interagency enforcement effort to prevent the dangerous and illicit transfer of the emerging technologies that will define our future. The Strike Force—which includes both a headquarters element as well as 14 cells throughout the United States in which prosecutors and agents from BIS, FBI, and Homeland Security Investigations work together—represents an effort to take a more concerted approach to investigating those who seek to exploit technology to undermine our national security.

Several recent prosecutions highlight this work. In May 2023, we arrested a Greek national for allegedly acquiring export-controlled technologies, including advanced electronics and equipment used in quantum cryptography and nuclear weapons testing, for Russia and serving as a procurement agent for its intelligence services. More recently, we brought charges against Russian nationals based in the United States and Canada who used corporate entities registered in New York City to unlawfully source and purchase millions of dollars' worth of dual-use electronics on behalf of companies affiliated with the Russian military. The targeted

technology included electronic components and integrated circuits with the same identifiers that have been found in Russian weapons and equipment seized in Ukraine.

D. Cyber, Economic Espionage, and Trade Secrets

Countries like China, Russia, Iran, and North Korea have accelerated their use of cyber capabilities to carry out activities that threaten our national security, such as by stealing sensitive technology, intellectual property, and personally identifiable information; using online means to exert malign influences upon our democracy; generating revenue to evade sanctions regimes; and holding our critical infrastructure at risk of destructive or disruptive attacks.

We have been proactive in counteracting nation-state efforts to use cyber-enabled means to undermine our security. In particular, we have worked in close partnership with the private sector to disrupt infrastructure deployed by nation-state actors through technical operations, such as the court-authorized takedowns of the Cyclops Blink botnet and the Snake malware network, each of which were used to malicious ends by the Russian intelligence services.

We also work to disrupt other cyber-enabled means to undermine our security. For example, in October 2023, we announced a series of disruptive actions against a network of North Korean IT workers who, posing as Western computer programmers, used online platforms to earn illegal revenue for North Korea's weapons programs from unsuspecting U.S. and other foreign companies. Through the seizure of fraudulent websites, asset freezes, threat intel sharing, and the related strengthening of anti-fraud measures, the U.S. government and private-sector partners disrupted this illicit revenue generation scheme.

Economic espionage and the theft of trade secrets are also critical priority for NSD, where our efforts are focused on combating our foreign state adversaries' efforts to steal cutting-edge and sensitive technologies by protecting companies where they are victims as well as prosecuting them when they facilitate such theft. As an example of the former, in May 2023, we charged two former software engineers with stealing software and hardware source code from U.S. companies in order to market it to Chinese competitors. The stolen code is alleged to be trade secrets used by the U.S. companies to develop self-driving cars and advanced automated manufacturing equipment. And as an example of the latter, in October 2020, a Taiwan-based semiconductor foundry company pleaded guilty to stealing a U.S. company's trade secrets relating to the design of circuits for memory chips used in computers and transferring them to a state-owned entity in China. The Taiwanese company was fined $60 million. The prosecution of the state-owned company is ongoing.

E. Foreign Investment Review

Nation-state adversaries increasingly seek to leverage strategic investment to access sensitive U.S. data and key technologies to the detriment of our national security. Within the Department, the National Security Division is responsible for assessing, mitigating, and preventing these national security and law enforcement risks.

NSD's Foreign Investment and Review Section proactively accomplishes this through its

participation in various interagency bodies and processes. As the Department's representative to the Committee on Foreign Investment in the United States (CFIUS), NSD helps to prevent foreign threat actors from exploiting investments to acquire U.S. assets and technology. NSD also reviews foreign participation in the telecommunications sector as chair of Team Telecom and works to secure the global supply chain for information and communications technology, software, and services in the United States through a variety of authorities.

When NSD cannot establish the fundamental trust required of compliance partners, we recommend through CFIUS that the President prohibit transactions or require divestment. More often, these review efforts involve working with companies to design and negotiate effective, verifiable, and monitorable national security mitigation measures. While collaboration and cooperation are critical to proactively addressing risks before they materialize, paper promises alone cannot resolve national security risks. NSD conducts ongoing monitoring to ensure companies uphold their commitments in the national security agreements and orders to which the Department is a party. NSD has many tools and approaches at its disposal to ensure compliance, such as CFIUS penalties, divestment, and referral of Team Telecom matters to the Federal Communications Commission's Enforcement Bureau or for criminal investigation.

F. Countering Foreign Malign Influence

Another key priority for NSD is countering efforts by nation states and other foreign actors to exert covert influence in the United States. Foreign state actors exploit modern technology and the increased inter-connectedness of our world to reach unprecedented numbers of Americans covertly and without ever setting foot on U.S. soil.

Critical to NSD's work to bolster transparency of foreign activities in the United States is our enforcement of the Foreign Agents Registration Act (FARA). FARA is a national security law designed to address covert efforts to influence policy and public opinion or to subvert our democracy by sowing division or otherwise distort the marketplace of ideas. FARA requires those acting as agents of foreign principals to disclose information about those relationships and appropriately label materials disseminated to the public. These requirements ensure that the American people and our lawmakers know and make informed decisions regarding the foreign source of information and activities intended to sway U.S. policymakers or the public.

FARA's transparency goals are key in countering nation-state threats at a time when foreign governments and foreign interests are increasing efforts to shape U.S. public policy. It is essential that corporate entities like sovereign wealth funds, law firms, or think tanks that work on behalf of foreign principals uphold FARA registration requirements. NSD enforces FARA administratively through voluntary compliance, civilly through cases filed in federal court for an injunctive order mandating compliance, and criminally for willful violations of the statute. But FARA currently lacks a mechanism to use civil investigative demand authority and impose civil monetary penalties for serious or repeat violations by corporate actors that do not rise to the level of a criminal violation. The Department supports legislative proposals to improve FARA compliance, including by creating additional intermediate civil enforcement tools which would better reflect the multi-dimensional relationship with corporate actors and would enable the Department to better incentivize corporate compliance with FARA. The Department is also in

the process of updating its FARA regulations to reflect changes in technology and the threat landscape.

III. The National Security Division's Approach to Corporate Enforcement and Compliance

As described above, the Department has changed its corporate enforcement policies to incentivize corporate responsibility and promote individual accountability—by clarifying and standardizing policies on voluntary self-disclosure and corporate cooperation and encouraging companies to potentially retool their compensation systems to promote compliance. The goal of the National Security Division's corporate enforcement program is to create the conditions for companies to invest in compliance programs that will prevent violations of our export control and sanctions laws, help them to detect violations that do occur, and report them to us.

We recognize that even the most well-designed and resourced compliance programs cannot prevent every violation of law, so when companies become aware that their employees may be committing crimes, we want the company to step up, report those facts to us, and help us to investigate and prosecute the individual offenders. To do that, NSD, like every Department component, has issued a policy that sets out how a company can obtain significantly more favorable treatment in a criminal investigation when it voluntarily self-discloses potentially criminal violations of our export control and sanctions laws.

As NSD's work demonstrates, our relationship with the business community is necessarily multi-faceted. Responsible corporate actors are critical to protecting our national assets and are on the front lines of sanctions and export control compliance efforts. Their decisions about which entities to do business with—and which entities to avoid—can often be just as impactful as our law enforcement disruptions or actions, and their cooperation and earlier reporting can be critical to our ability to identify and punish violations.

The bottom line is that we need responsible corporate actors to join us in the fight to defend U.S. national security. Certainly, when investigations of corporate crime reveal violations of our national security laws, and where companies violate the law, we will continue to hold them accountable. But we do not measure the effectiveness of our corporate enforcement efforts simply by the number of cases we bring. Rather, we judge our progress in this area by the impact of our efforts to protect the national security of the United States—both through our own efforts and interagency partnership with Treasury, Commerce, and State Departments.

IV. Challenges

Corporate investigations are complex, time-consuming matters that require the investment of significant resources to conduct effectively. Indeed, many of the National Security Division's recent corporate enforcement cases have involved the collection and review of millions of documents and the need to navigate the complex legal and logistical challenges inherent to conducting cross-border investigations.

To meet this challenge, NSD is committing significant new resources to bolster our

approach to corporate enforcement. Over the past year, we have added more than 25 new prosecutors to work on sanctions evasion, export control violations, and other similar cases. And in September, NSD announced the appointments of two veteran prosecutors to be the first Chief Counsel and Deputy Chief Counsel for Corporate Enforcement, to lead and oversee NSD's investigation and prosecution of national security-related corporate crime.

As NSD expands its capacity to investigate and prosecute corporate violations of national security laws, it will continue to work closely with U.S. Attorney's Offices and the Criminal Division to apply enforcement strategies that have proven their worth in other areas of the Department. In this effort, we can draw upon lessons learned from the success of the Criminal Division's enforcement efforts.

* * *

As we respond to a dynamic and evolving threat landscape, we will remain committed to using all the legal authorities in our arsenal to defend the nation against threats from state and non-state adversaries. When companies commit crimes that undermine our national security, we will be relentless in pursuing them. The Department is committed to ensuring individual accountability, discouraging corporate recidivism, promoting strong corporate culture, encouraging voluntary self-disclosure, and promoting transparency and public confidence.