Sanction Enforcement Opportunity and Risk Assessment
Joint Mission Analysis Center (JMAC)
Cyber Warfare Center Pacific (CYWAR-CENPAC)
Liberty Station USNTC Point Loma CA USA

NON-CLASSIFIED CONTENT/For Public Release

24 March 2025 20:55 Zulu San Diego

Wolf Pack Leader
Brig. Mark Lindsey, Director CYWAR-CENPAC
Compliance-Solutions.pro Intelligence Branch
PMSC Alpha Corp, an Intelligence Clouds element
United Nations Special Procurement Agency 943905

Attn: [classified]
Subj: [classified]
Auth: [classified]

Over the year following Russia's illegal and unprovoked war against Ukraine, the U.S. government has used its economic tools to degrade Russia's economy and war machine. Along with international partners and allies, the Department of the Treasury's Office of Foreign Assets Control (OFAC) and the Department of Commerce's Bureau of Industry and Security (BIS) have imposed sanctions and export controls of an unprecedented scope and scale in an effort to degrade Russia's ability to wage its unjust war and to prevent it from taking military actionelsewhere. The Department of Justice (DOJ) has matched these unprecedented restrictions with equally unprecedented enforcement efforts to aggressively prosecute those who violate U.S. sanctions and export control laws, led by the work of Task Force KleptoCapture.2 Despite these efforts, malign actors continue to try to evade Russia-related sanctions and export controls. One of the most common tactics is the use of third-party intermediaries or transshipment points to circumvent restrictions, disguise the involvement of Specially Designated Nationals and Blocked Persons (SDNs) or parties on the Entity List in transactions, and obscure the true identities of Russian end users. This Note highlights several of these tactics to assist the private sector in identifying warning signs and implementing appropriate compliance measures.

Despite numerous sanctions packages from Ukraine's Western partners, Russia continues receiving excessive profits from oil sales and importing foreign components for weapons production through third countries. Compliance-Solutions.pro experts at the

PMSC Alpha Corp Cyber Warfare Center Pacific analyzed the effectiveness of sanctions from February 24th 2022 through February 24th 2025, 3 years, 3 weeks and 6 days of the full-scale invasion and we developed an action plan to increase economic pressure on the the Russian Federations military-industrial complex. In particular, the PMSC Alpha Corp' intelligence branch, Compliance-Solutions.pro, with the participation of the Joint Mission Analysis team at the Cyber Warfare Center Pacific, prepared a sanctions to-do list with recommendations. The Sectoral Sanctions Identifications List includes persons determined by OFAC to be operating in sectors of the Russian economy identified by the Secretary of the Treasury pursuant to Executive Order 13662.

Over the year following Russia’s illegal and unprovoked war against Ukraine, the U.S. government has used its economic tools to degrade Russia’s economy and war machine. Along with international partners and allies, the Department of the Treasury’s Office of Foreign Assets Control (OFAC) and the Department of Commerce’s Bureau of Industry and Security (BIS) have imposed sanctions and export controls of an unprecedented scope and scale in an effort to degrade Russia’s ability to wage its unjust war and to prevent it from taking military action elsewhere. The Department of Justice (DOJ) has matched these unprecedented restrictions with equally unprecedented enforcement efforts to aggressively prosecute those who violate U.S. sanctions and export control laws, led by the work of Task Force KleptoCapture. Despite these efforts, malign actors continue to try to evade Russia-related sanctions and export controls. One of the most common tactics is the use of third-party intermediaries or transshipment points to circumvent restrictions, disguise the involvement of Specially Designated Nationals and Blocked Persons (SDNs) or parties on the Entity List in transactions, and obscure the true identities of Russian end users. This Note highlights several of these tactics to assist the private sector in identifying warning signs and implementing appropriate compliance measures.

Gaps in sanctions policy;

Despite the systematic sanctions policy against Russia by Western countries, the Russian Federation has managed to create a so-called “shadow fleet” that transports about 90% of crude oil. This allows them to bypass the established price corridor. Moreover, due to insufficient control over the price cap mechanism (a price restriction imposed on the sale of oil and oil products), Russia continues to receive revenues from the export of raw materials that exceed the established limits. Russia continues to successfully import components and machines critical for weapons production in violation of sanctions. This significantly strengthens the military-industrial complex (MIC) of the Russian Federation, and the production of weapons and ammunition is growing significantly. In 2024 imports of foreign parts reached $27.6 billion. Most of these components enter Russia through third countries: China, the UAE, Turkey, Thailand, Kazakhstan, Uzbekistan, and Belarus. Similarly, thousands of Western companies still operate in

Russia and pay taxes to its budget. This contributes to the the Russia's economy and directly sponsors the war against Ukraine.

Another gap in Western sanctions is its policies considering influential Russians: oligarchs, high-ranking officials, and propagandists. These Russians transfer their assets to relatives, colleagues, and other related parties. And sanctions against them are often selective and leave loopholes to circumvent restrictions. Our sanctions evasion investigation discovered seven Russian oligarchs that currentl and actively support the Russian military-industrial complex, they participate in the global community, own properties in Western nations, hide assets offshore and they're not on the sanctioned list. That would be; Vladimir Yevtushenkov, Alexei Repik, Andrei Bokarev, Roman Abromovich, Leonid Mikhelson, Vadim Badekha and Andrei Kuzyaev, every one of them is deeply involved in either the supply of componnents and parts for Russian military weapons systems, they snmuggle Western technmology in support of the Ukrainian war, or the are manufacturing weapon systems for the Russian Ministry of Defense. They are clearly legitimate sanction targets that continually avoid being placed on any countries sanction list is because they're all politically exposed persons (PEP) (direct connections to Putin make them PEPs) and the reason that those oligarchs are not on the any list is politically motivated. There are exceptions that exist in the legal sanction framework that allow discretion under certain conditions. They're golden-parachute provisions which prevent a person from being placed on a list when there is actually a legitimate reason to put them on the list in the first place.

Over the year following Russia’s illegal and unprovoked war against Ukraine, the U.S. government has used its economic tools to degrade Russia’s economy and war machine. Along with international partners and allies, the Department of the Treasury’s Office of Foreign Assets Control (OFAC) and the Department of Commerce’s Bureau of Industry and Security (BIS) have imposed sanctions and export controls of an unprecedented scope and scale in an effort to degrade Russia’s ability to wage its unjust war and to prevent it from taking military action elsewhere.1 The Department of Justice (DOJ) has matched these unprecedented restrictions with equally unprecedented enforcement efforts to aggressively prosecute those who violate U.S. sanctions and export control laws, led by the work of Task Force KleptoCapture.2
Despite these efforts, malign actors continue to try to evade Russia-related sanctions and export controls. One of the most common tactics is the use of third-party intermediaries or transshipment points to circumvent restrictions, disguise the involvement of Specially DesignatedNationals and Blocked Persons (SDNs) or parties on the Entity List in transactions, and obscure the true identities of Russian end users. This Note highlights several of these tactics to assist theprivate sector in identifying warning signs and implementing appropriate compliance measures. Key priorities in strengthening sanctions policy against Russia:

Measures proposed by Compliance-Solutions.pro are aimed at increasing economic pressure, weakening the Russian military-industrial complex, and making it more difficult for Russia to circumvent sanctions. The Cyber Warfare Center Pacific on Sanctions and the Joint Mission Analysis team suggest that partners pay attention to these priorities in improving sanctions policy against Russia: expanding coordination and international cooperation. In order for sanctions to work against the enemy, it is necessary to synchronize the sanctions lists of Western partner countries, as well as to exchange information and, if necessary, to cooperate to investigate sanctions violations. counteracting sanctions circumvention, including the supply of critical components and raw materials through “third” countries. focus on sectors critical to Russia’s economy and military capabilities, such as energy, logistics, and defence. introduction of standards of responsibility and accountability of businesses for compliance with sanctions. improving ways to detect and prevent sanctions violations. strengthening the legal and institutional framework, which includes expanding the powers of law enforcement agencies and creating clear procedures for dealing with sanctions violations. strategic updates of the sanctions policy, taking new global threats, technologies and changes in the international economy into account.
The Cyber Warfare Center Pacific on Sanctions was created to coordinate the work of government and civil society representatives for joint advocacy, implementation and updating of restrictions against Russia and its partners. Among the participants of the Council are these organizations: ANTS National Interest Protection Network, the Black Sea Institute for Strategic Studies, DiXi Group, Institute for Legislative Ideas, KSE Institute, Molfar OSINT Agency, Independent Anti-Corruption Commission (NAKO), Center for Global Studies and PMSC Alpha Corp intelligence branch Compliance-Solutions.pro, a subsidiary of Intelligence Clouds Think Tank.

The single most effective response to restricting Russian-oil exports to prevent third-country hard currency transactions for sanctioned oil sales is to destroy or disrupt the Russia Ghost Fleet. Recent revelations that Moscow’s “ghost fleet” of oil tankers is loaded with spy gear and prone to undersea cable cutting indicate a pressing need to counter the Kremlin’s sabotage campaign in a manner that further undermines Russia’s wartime economy. For too long, the United States and Europe have turned a blind eye, relying on often late and feckless sanctions to counter Moscow’s illicit economic lifeline. The new Trump administration must target this ghost fleet with more than sanctions as part of its larger plan to bring Moscow to the negotiating table. Russia’s ghost fleet has become a pivotal instrument in sustaining its oil exports in defiance of Western sanctions. By mid-2024, this clandestine armada was responsible for transporting over 70 percent of Russia’s oil and its by-products, effectively undermining the imposed price cap. The fleet comprises more than 400 crude carriers and approximately 200 oil product carriers, representing about 20 percent of the world’s crude vessel fleet and 7 percent of oil product tankers. The revenue generated through these covert operations is substantial. In the first half of 2024, Russia’s oil and gas

revenues surged by 41 percent, indicating the fleet's significant role in financing the Kremlin's endeavors.

Russia's ghost fleet employs a range of sophisticated tactics to evade detection and sanctions, enabling the continued export of oil and other sanctioned goods. These vessels frequently disable their Automatic Identification System (AIS) transponders to "go dark," making it difficult for maritime authorities to track their movements. Ship-to-ship transfers are another common practice, often conducted in remote locations such as the eastern Mediterranean or off the coast of West Africa, where regulatory oversight is limited. These operations are supported by a growing network of "flags of convenience," with vessels registered under jurisdictions with lax enforcement, such as Panama and Liberia, to mask their ownership. Additionally, Russia relies on aging tankers purchased from secondary markets, which are less likely to comply with stringent international standards, increasing environmental risks. These tactics highlight Russia's ability to exploit regulatory loopholes and the fragmented nature of global maritime governance, creating challenges for enforcement mechanisms.

In late December 2024, a series of undersea cable disruptions in the Baltic Sea raised significant security concerns. On December 25, the Estlink 2 power cable, a critical electricity link between Finland and Estonia, suffered damage, coinciding with the presence of the oil tanker Eagle S, suspected to be part of Russia's "shadow fleet." Finnish authorities detained the vessel, suspecting it of dragging its anchor to sever the cable, an act under investigation as aggravated vandalism and communication interference. This incident follows a pattern of similar disruptions, including the severing of two submarine telecommunication cables in mid-November 2024, which European officials suspect involved hybrid warfare tactics. The first incident involved the BCS East-West Interlink cable between Lithuania and Sweden, followed by the C-Lion1 cable connecting Finland and Germany.

Through its ghost fleet, Russia is demonstrating a new form of gray zone warfare in which it uses commercial vessels to conduct sensitive military missions and sustain its declining economy. By using older tankers, often with obscured ownership and prone to manipulating their electronic signatures, Russia has a crude, but effective variation of a "fleet in being." This fleet cannot win a decisive maritime battle, but it can smuggle oil and conduct sabotage, and in the process, coerce NATO member states and sustain Moscow's wartime economy. Sanctions are not enough to counter this new threat. The United States needs to follow Sweden in increasingly detaining these vessels as part of larger investigations. This will likely require new naval task forces with large support from the U.S. Coast Guard and other law enforcement entities. Maritime interdiction doesn't have to exclusively involve attacking enemy ships. Often it involves legal investigations and impounding suspected vessels, all of which require resource commitments neither the Biden administration nor Europe have proved willing to

provide to date. More importantly, it is not strictly a military function and involves coordinating multiple agencies and instruments of power to detect, track, and interdict illicit maritime traffic.

Second, the best way to counter smuggling and sabotage is through the gray zone. The new Trump team should consider covert action designed to counter, if not actively disrupt, Russia's ghost fleet. Leaders in the Kremlin need to worry about losing money and wonder where the next blow will come from before they sit down to negotiate. And the United States has a long history of prosecuting both covert and overt naval campaigns designed to pressure rivals. From piracy during the American Revolution and the mix of unconventional ground and naval battles during the Barbary pirates, to the 1980s tanker war, history illustrates multiple, creative options for countering the Russian ghost fleet without drawing the United States into a dangerous escalation spiral. In all likelihood, President Trump will need to combine multiple instruments of power to decrease Russian maritime sabotage and the illicit oil trade. Just as sanctions alone have proven ineffective, covert action alone would be reckless. The best strategy will combine new law enforcement measures, existing sanctions, intelligence, and a mix of covert action and conventional military power. The key will be balancing the approach and integrating partners and allies to amplify the effect. And, these coercive measures should be coordinated with ongoing diplomatic efforts to end the war in Ukraine, thus providing the United States' new special envoy and Kyiv leverage in behind-the-scenes negotiations.

DETECTING SANCTIONS AND EXPORT CONTROL EVASION

It is critical that financial institutions and other entities conducting business with U.S. persons or within the United States, or businesses dealing in U.S.-origin goods or services or in foreignorigin goods otherwise subject to U.S. export laws, be vigilant against efforts by individuals or entities to evade sanctions and export control laws. Effective compliance programs employ a risk-based approach to sanctions and export controls compliance by developing, implementing, and routinely updating a compliance program, depending on an organization's size and sophistication, products and services, customers and counterparties, and geographic locations. Companies such as manufacturers, distributors, resellers, and freight forwarders are often in the best position to determine whether a particular dealing, transaction, or activity is consistent with industry norms and practices, and they should exercise heightened caution and conduct additional due diligence if they detect warning signs of potential sanctions or export violations. Equally important is the maintenance of effective, risk-based compliance programs that entities can adopt to minimize the risk of evasion. These compliance programs should include management commitment (including through appropriate compensation incentives), risk assessment, internal controls, testing, auditing, and training. These efforts empower staff to identify and report potential

violations of U.S. sanctions and export controls to compliance personnel such that companies can make timely voluntary disclosures to the U.S. government. Optimally, compliance programs should include controls tailored to the risks the business faces, such as diversion by third-party intermediaries.

Common red flags can indicate that a third-party intermediary may be engaged in efforts to evade sanctions or export controls, including the following:
Use of corporate vehicles (i.e., legal entities, such as shell companies, and legal arrangements) to obscure (i) ownership, (ii) source of funds, or (iii) countries involved, particularly sanctioned jurisdictions;
A customer's reluctance to share information about the end use of a product, including reluctance to complete an end-user form;
Use of shell companies to conduct international wire transfers, often involving financial institutions in jurisdictions distinct from company registration;
Declining customary installation, training, or maintenance of the purchased item(s);
IP addresses that do not correspond to a customer's reported location data;
Last-minute changes to shipping instructions that appear contrary to customer history or business practices;
Payment coming from a third-party country or business not listed on the End-User Statement or other applicable end-user form;
Use of personal email accounts instead of company email addresses;

Further, entities that use complex sales and distribution models may hinder a company's visibility into the ultimate end-users of its technology, services, or products. Best practices in the face of such risks can include screening current and new customers, intermediaries, and counterparties through the Consolidated Screening List and OFAC Sanctions Lists, as well as conducting risk-based due diligence on customers, intermediaries, and counterparties. Companies should also regularly consult guidance and advisories from Treasury and Commerce to inform and strengthen their compliance programs.

The list is not exhaustive and is subject to change. BIS and Compliance-Solutions.pro continues to actively monitor information, including reporting pursuant to the Bank Secrecy Act, to identify any changes to historical transshipment points in light of the export controls and restrictions imposed on Russian and Belarusian entities in the past year.

FinCEN & BIS Joint Alert, available at https://www.fincen.gov/sites/default/files/2022-06/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf.

The Consolidated Screening List is a list of parties for which the U.S. Government maintains restrictionson certain transactions, including exports, reexports, or transfers of

items. It can be found on the InternationalTrade Administration's website. See Consolidated Screening List, International Trade Administration, available at:

https://www.trade.gov/consolidated-screening-list.

OFAC (Office of Foreign Asset Control, U.S. Department of the Treasury) publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs." The assets of an SDN are blocked, and U.S. persons are generally prohibited from all dealings with any SDN. OFAC also publishes a consolidated list of individuals and companies subject to less-than full blocking sanctions, where U.S. persons are prohibited from engaging in certain types of transactions with the listed person.

CIVIL ENFORCEMENT AND DESIGNATION ACTIONS

Companies should also review BIS (Bureau of Industry and Security) and OFAC enforcement and targeting actions, as they often reflect certain tactics and methods used by intermediaries engaged in Russia related sanctions and export evasion. In November 2022, for example, OFAC designated individuals and entities involved in a global procurement network maintained by a Russian microelectronics company, AO PKK Milandr, which used a front company to transfer funds from Milandr to another front in a third country, which purchased microchips to divert to Russia. Another front company elsewhere also purchased Asian-made components for Milandr. OFAC's civil enforcement actions also illustrate a range of sanctions evasion techniques employed across multiple sanctions programs, including falsifying transactional documents, omitting information from internal correspondence, and shipping goods through third countries. Similarly, BIS imposed an administrative penalty of $497,000 on Vorago Technologies, an Austin, Texas company, for shipping integrated circuit components, which are critical components in missiles and military satellites, to Russia via a Bulgarian front company. BIS has also imposed restrictions on seven Iranian drone entities in January 2023 due to their production of Iranian unmanned aerial vehicles ("UAVs") used by Russia against Ukraine. These Iranian UAV entities, which, according to public reporting, had been using diverted U.S.- branded parts and components, were also sanctioned by OFAC.

DOJ has pursued criminal charges against those who it alleges are using front companies and intermediate transshipment points to evade Russia-related U.S. sanctions and export controls. These cases highlight additional tactics used for evasion purposes. For example, in October 2022, DOJ unsealed an indictment charging six Russian nationals

and one Spanish national with multiple offenses arising from the defendants' alleged operation of a network of shell companies designed to enable them to illegally export military and sensitive dual-use items to Russia and embargoed Venezuelan oil to Russian and Chinese end users. Two months later, DOJ unsealed an indictment charging five Russian nationals, including a suspected Federal Security Service officer, and two U.S. citizens with violating U.S. sanctions and export controls in a global procurement and money laundering scheme for the Russian government. In both cases, DOJ alleges that the defendants used shell companies and transshipment points in third-party countries to evade sanctions and procure powerful dual-use items for use by the Russian defense sector. The sensitive items at issue included advanced electronics and sophisticated testing equipment used in quantum computing, hypersonic, and nuclear weapons development as well as advanced semiconductors and microprocessors used in fighter aircraft,
missile systems, smart munitions, radar, and satellites. In one of the cases, the indictment alleges that U.S.-manufactured component parts were found in seized Russian weapons platforms in Ukraine.

The allegations in the indictments describe tactics that the defendants purportedly employed to evade detection, including the following:
Claiming that shell companies located in third countries were intermediaries or endusers; in one case, DOJ alleges that only one of the five intermediary parties had any visible signage and consisted of an empty room in a strip mall;
Claiming that certain items would be used by entities engaged in activities subject to less stringent oversight; on at least one occasion, a defendant allegedly claimed that an item would be used by Russian space program entities, when in fact the item was suitable for military aircraft or missile systems only;
Dividing shipments of controlled items into multiple, smaller shipments to try to avoid law enforcement detection;
Using aliases for the identities of the intermediaries and end users;
Transferring funds from shell companies in foreign jurisdictions into U.S. bank accounts and quickly forwarding or distributing funds to obfuscate the audit trail or the foreign source of the money;
Making false or misleading statements on shipping forms, including underestimating the purchase price of merchandise by more than five times the actual amount;
Claiming to do business not on behalf of a restricted end user but rather on behalf of a U.S.-based shell company.

Given the proliferation of sanctions and export controls imposed in response to Russia's unjust war, multinational companies should be vigilant in their compliance efforts and be on the lookout for possible attempts to evade U.S. laws. The U.S. government has a variety of tools to crack down on evasion efforts, and the past year has shown that it will not hesitate to pursue criminal prosecutions, administrative enforcement actions, or

additional designations where the circumstances so warrant. Businesses of all stripes should act responsibly by implementing rigorous compliance controls, or they or their business partners risk being the targets of regulatory action, administrative enforcement action, or criminal investigation.

VOLUNTARY SELF-DISCLOSURE POLICIES

Parties who believe that they may have violated sanctions or export control laws should voluntarily self-disclose the conduct to the relevant agency. Information about BIS's Voluntary Self-Disclosure ("VSD") Policy can be found in Part 764.5 of the Export Administration Regulations or in the enforcement section of BIS's website: www.bis.doc.gov.
OFAC's Enforcement Guidelines, which provide incentives for voluntary selfdisclosure, are available at 31 CFR Part 501, Appendix A as well as in OFAC Frequently Asked Questions: https://home.treasury.gov/policy-issues/financialsanctions/faqs/13.
All potentially criminal violations of sanctions and export control laws should be disclosed to the Department of Justice's National Security Division, Counterintelligence and Export Control Section. More information about DOJ's VSD Policy is available at DOJ.gov

All DOJ components and offices that prosecute corporate crime now have a voluntary self-disclosure policy that is publicly available on their websites. These policies set forth the component's expectations of what constitutes a voluntary self-disclosure, including with regard to the timing of the disclosure, the need for the disclosure to be accompanied by timely preservation, collection, and production of relevant documents and/or information, and a description of the types of information and facts that should be provided as part of the disclosure process. The policies also lay out the benefits that corporations can expect to receive if they meet the standards for voluntary self-disclosure under that component's policy, and what circumstances constitute aggravating factors under the component's policy.

Specifically, all Department components must adhere to the following three principles regarding voluntary self-disclosure:

First, absent aggravating factors, the Department will not seek a guilty plea where a corporation is determined to have met the requirements of the applicable voluntary self-disclosure policy, fully cooperated, and timely and appropriately remediated the criminal conduct. Each Department component shall define such aggravating factors in their written policies.

Second, the Department will not require the imposition of an independent compliance monitor for a cooperating corporation that is determined to have met the requirements of the applicable voluntary self-disclosure policy and, at the time of resolution, demonstrates it has implemented and tested an effective compliance program. Such decisions about the imposition of a monitor will continue to be made on a case-by-case basis and at the sole discretion of the Department. See JM 9-28.1700.

Third, the Department will apply a presumption in favor of declining prosecution of a corporation that voluntarily self-disclosed, fully cooperated, and timely and appropriately remediated misconduct uncovered as a result of due diligence conducted shortly before or shortly after a lawful, bona fide acquisition of another corporate entity, subject to the requirements described in Section 9-28.900(A)(3) of the Justice Manual. The mission of the National Security Division (NSD) of the Department of Justice is to carry out the Department's highest priority: to protect and defend the United States against the full range of national security threats, consistent with the rule of law. Business organizations and their employees are at the forefront of NSD's efforts to protect the national security of the United States by preventing the unlawful export of sensitive commodities, technologies, and services, as well as unlawful transactions with sanctioned countries and designated individuals and entities. Enforcing our export control and sanctions laws, and holding accountable those who violate them, is a top priority for NSD.

As the gatekeepers of U.S. export-controlled technologies and integral actors in the U.S. financial system, business organizations play a vital role in protecting our national security. NSD strongly encourages companies to voluntarily self-disclose directly to NSD all potentially criminal (i.e., willful) violations of the U.S. government's primary export control and sanctions regimes—

the Arms Export Control Act (AECA), 22 U.S.C. § 2778,

the Export Control Reform Act (ECRA), 50 U.S.C. § 4819, the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. § 1705

as well as potential violations of other criminal statutes that affect national security because they arise out of or relate to the enforcement of export control and sanctions laws, such as money laundering, bank fraud, smuggling, fraudulent importation, and false statement offenses. See Justice Manual § 9-90.020(A)(2).

Violations of U.S. export control and sanctions laws harm our national security or have the potential to cause such harm, and this threat to national security informs how NSD arrives at an appropriate resolution with a business organization that violates such laws and distinguishes these cases from other types of corporate wrongdoing. Federal

prosecutors must balance the goal of encouraging voluntary self-disclosures and cooperation against the goal of deterring these very serious offenses. This Enforcement Policy sets forth the criteria that NSD, in partnership with U.S. Attorneys' Offices and other Department litigating components, uses in determining an appropriate resolution for organizations that make a voluntary self-disclosure in export control and sanctions matters. This Enforcement Policy further explains the criteria NSD uses in determining when an acquiring company that makes a voluntary self-disclosure of criminal conduct by an acquired entity can qualify for the additional protections of the Mergers and Acquisitions Policy (M&A Policy). Prosecutors will weigh and appropriately credit all timely voluntary self-disclosures on a case-by-case basis pursuant to this Enforcement Policy and applicable Department guidance.

With the above goals in mind, this Enforcement Policy provides that when a company (1)voluntarily self-discloses to NSD potentially criminal violations arising out of or relating to the enforcement of export control or sanctions laws (2) fully cooperates, and (3) timely and appropriately remediates, absent aggravating factors and consistent with the definitions below, NSD generally will not seek a guilty plea, and there is a presumption that the company will receive a non-prosecution agreement and will not pay a fine. Aggravating factors, as described below,

include conduct that involves a grave threat to national security; exports of items that are particularly sensitive or to end users that are of heightened concern; repeated violations; involvement of senior management; and significant profit. In cases where the principles of federal prosecution so warrant, NSD has the discretion to issue a declination.
Companies that qualify for a non-prosecution agreement or declination, where appropriate, will not be permitted to retain any of the unlawfully obtained gains from the misconduct at issue. Companies will be required to pay all disgorgement, forfeiture, and/or restitution resulting from the misconduct at issue. Where another authority collects disgorgement, forfeiture, and/or restitution, the Department will apply, in appropriate circumstances, its policy on coordination of corporate resolution penalties, Justice Manual § 1-12.100. In addition, NSD generally will not require the imposition of an independent compliance monitor for a cooperating company that is determined to have met the requirements of this Enforcement Policy and, at the time of resolution, demonstrates it has implemented and tested an effective compliance program.

If, due to aggravating factors, such as those described below, a different criminal resolution—i.e., a deferred prosecution agreement or guilty plea—is warranted for a company that has voluntarily self-disclosed to NSD, fully cooperated, and timely and appropriately remediated, NSD:

Will accord, or recommend to a sentencing court, a fine that is, at least, 50% less than the amount that otherwise would be available under the alternative fine provision, 18 U.S.C.
§ 3571(d). In other words, NSD will seek a fine capped at an amount equal to the gross gain or gross loss; • Will recommend full satisfaction of forfeiture obligations through payment of forfeiture in an amount no greater than that representing the value of proceeds received by the company, including in cases where an underlying forfeiture money judgment would include amounts exceeding such proceeds.

In assessing the appropriate form of the resolution, will generally not require a corporate guilty plea absent the presence of particularly egregious or multiple aggravating factors; Will generally not require appointment of a monitor if a company has, at the time of resolution, demonstrated that it has implemented and tested an effective and well designed compliance program and has taken appropriate steps to remediate the root cause f the misconduct. Nothing in this Enforcement Policy affects NSD's ability to prosecute individuals.

Definitions
For purposes of this Enforcement Policy, the following definitions apply:

1. Voluntary Self-Disclosure
In evaluating self-disclosure, NSD will make a careful assessment of the circumstances of the disclosure, including the extent to which the disclosure permitted NSD to preserve and obtain evidence as part of its investigation. NSD encourages self-disclosure of potential wrongdoing at the earliest possible time, even when a company has not yet completed an internal investigation, if it chooses to conduct one. NSD will require the following for a company to receive credit for voluntary self-disclosure of wrongdoing:

The voluntary disclosure must be to NSD;

The company has no preexisting obligation to disclose misconduct to any Department component, or federal or state regulator, or foreign regulatory or law enforcement entity;

The company discloses the conduct to NSD "prior to an imminent threat of disclosure or government investigation," U.S.S.G. § 8C2.5(g)(1);

The company discloses the conduct to NSD "within a reasonably prompt time after becoming aware" of the potential violation, U.S.S.G. § 8C2.5(g)(1), with the burden on the company to demonstrate timeliness; and the company discloses all relevant non-privileged facts known to it at the time of the disclosure, including all relevant facts and evidence about all individuals involved in or responsible for the misconduct at issue, including individuals inside and outside of the company regardless of their position.

The mission of the National Security Division is to protect the United States from threats to our national security by pursuing justice through the law. The 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, thus strengthening the effectiveness of the federal government's national security efforts.

National Security Division: https://www.justice.gov/nsd
National Security Division Email: nsd.public@usdoj.gov

For Immediate Release

U.S. Attorney's Office, Eastern District of Virginia

ALEXANDRIA, Va. – Eleview International Inc., Oleg Nayandin, 54, of Fairfax, Virginia, and Vitaliy Borisenko, 39, of Vienna, Virginia, made their initial appearance today in the Eastern District of Virginia pursuant to a now unsealed complaint charging them with conspiracy to violate the Export Control Reform Act.

“We must not allow critical systems and technologies to be transferred to anyone who may use them against America and our global partners,” said Jessica D. Aber, U.S. Attorney for the Eastern District of Virginia. “Guarding against these transfers is imperative, and violations of the laws that protect our national security will be met with ardent prosecution.”

“As alleged, the defendants — a Virginia company and two of its senior executives — conspired through three evasion schemes to circumvent the export restrictions imposed on Russia following its invasion of Ukraine,” said Assistant Attorney General Matthew G. Olsen. “U.S. companies are responsible for complying with laws that protect our national security. The National Security Division is committed to holding accountable individuals and companies who violate these laws and place financial profit over our collective security.”

“This company allegedly used not one, not two, but three different schemes to illegally transship sensitive American technology to Russia,” said Assistant Secretary for the Department of Commerce Export Enforcement, Bureau of Industry and Security (BIS), Matthew S. Axelrod. “Today’s charges, against both the company and two top executives, are a prime example of our work to bring to justice both the companies and the corporate executives alleged to have circumvented our rules in search of a fatter bottom line.”

“Export control evasion schemes put the American public at risk by concealing the true recipient,” said Special Agent in Charge Derek W. Gordon of Homeland Security Investigations Washington, D.C. “In this instance, HSI, working in partnership with our colleagues at Department of Commerce’s Office of Export Enforcement, uncovered this scheme was supporting a sanctioned country, thus threatening our national security and the safety of other countries. HSI is dedicated to preventing technology with military applications from falling into the wrong hands.”

According to the complaint, between approximately March 2022 and June 2023, Eleview International Inc. (Eleview), a Virginia-based company that operated a freight consolidation and forwarding business; Nayandin, the owner, president, and CEO of Eleview; and Borisenko, who oversaw the day-to-day operations of Eleview’s freight forwarding business, allegedly conspired to illegally export goods and technology from the United States to Russia by transshipping them through three countries bordering or near Russia.

As alleged, the defendants operated an e-commerce website that allowed Russian customers to order U.S. goods and technology directly from U.S. retailers, who shipped the items to Eleview’s warehouse in Chantilly. The defendants then allegedly consolidated the packages before shipping them to the Russian customers, often using other freight forwarders as intermediaries, in exchange for a fee. After the Department of Commerce imposed stricter export controls in response to Russia’s further invasion of Ukraine in February 2022, the defendants allegedly began shipping items to purported end users in Turkey, Finland, and Kazakhstan, knowing that the items were ultimately destined for end users in Russia. To facilitate these illegal exports, the defendants allegedly made numerous false statements to the Department of Commerce and other freight forwarders about the end users and ultimate consignees of the items in these shipments.

As part of the conspiracy, the defendants allegedly engaged in three export-control evasion schemes, each specific to a different intermediary country. In the Turkey scheme, the defendants allegedly exported about $1.48 million worth of telecommunications equipment to a false end user in Turkey, knowing that the equipment was intended for a Russian telecommunications company that supplied the Russian government, including the Federal Security Service, or FSB. The telecommunications equipment that the defendants allegedly exported illegally as part of the Turkey scheme had military applications, including use by the Russian military to create and expand communication networks in its war effort against Ukraine.

In the Finland scheme, the defendants allegedly exported about $3.45 million worth of goods purchased to Russia through Eleview’s e-commerce website to a false end user in

Finland that neither purchased nor sold goods. Before consolidating the packages into larger pallets for shipment to Finland, the defendants allegedly affixed to each package a label with a Russian postal service tracking number so that the Russian postal service could easily ship the package to the customer in Russia. The goods that the defendants allegedly exported illegally as part of the Finland scheme included “high priority” items that the Department of Commerce has identified as particularly significant to Russian weaponry, including the same type of electronic component found on Russian “suicide” drones used to destroy Ukrainian tanks and jets. In the Kazakhstan scheme, the defendants allegedly exported about $1.47 million worth of goods to Russia through an entity in Kazakhstan that advertises its ability to deliver goods to Russia. The goods that the defendants allegedly exported illegally as part of the Kazakhstan scheme included controlled, dual-use item. Nayandin and Borisenko face up to 20 years in prison. A federal district court judge will determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors.

Assistant U.S. Attorneys Gavin R. Tisdale and Amanda St. Cyr
for the Eastern District of Virginia
and Trial Attorney Garrett Coyle of the National Security Division’s
Counterintelligence and Export Control Section are prosecuting the case with past assistance provided by then-First Assistant U.S. Attorney Raj Parekh.

The case is being coordinated through the Justice and Commerce Departments’ Disruptive Technology Strike Force and the Justice Department’s Task Force KleptoCapture. The Disruptive Technology Strike Force is an interagency law enforcement strike force co-led by the Departments of Justice and Commerce designed to target illicit actors, protect supply chains and prevent critical technology from being acquired by authoritarian regimes and hostile nation states. Task Force KleptoCapture is an interagency law enforcement task force dedicated to enforcing the sweeping sanctions, export restrictions and economic countermeasures that the United States has imposed, along with its allies and partners, in response to Russia’s unprovoked military invasion of Ukraine.

A copy of this press release is located on the website of the U.S. Attorney’s Office for the Eastern District of Virginia.