EIB World Trade Headlines

Evolutions In Business • www.eib.com • (978) 256-0438
Fax: (978) 250-4529 • P.O. Box 4008, Chelmsford, MA 01824

August 1, 2024 - Volume 19, Issue 15

FOR IMMEDIATE RELEASE
July 29, 2024
www.bis.gov

BUREAU OF INDUSTRY AND SECURITY
Office of Congressional and Public Affairs
OCPA@bis.doc.gov

Military and Intelligence End Uses and End Users
Publication Date: 07-29-2024
Comments due: 09-27-2024
The regulations.gov ID for this rule is: BIS–2024–0029.
Please refer to RIN 0694–AJ43 in all comments.
89 FR 60985

The Department of Commerce, Bureau of Industry and Security (BIS), seeks public comment on proposed changes to existing restrictions under the Export Administration Regulations (EAR) on military and intelligence end uses and end users and related U.S. persons activities controls, as well as the proposed addition of a military-support end-user control. These proposed revisions and additions to the EAR's end-use, end-user, and "U.S. persons" activity controls would implement expanded Export Control Reform Act of 2018 (ECRA) authority to control certain "U.S. persons" activities under the EAR. Specific to the EAR's "U.S. persons" activities controls, BIS is proposing amendments to control 'support' furnished by "U.S. persons" to military end users and military-production activities, as well as intelligence end users that are not otherwise already regulated under or prohibited by U.S. law. In addition, BIS is proposing to revise the definition of 'support' set forth in the EAR's "U.S. person" activity control provision in response to requests by the public for clarification. The revisions and additions, along with clarifications, to end use, end user, and "U.S. persons" activity controls under the EAR, would further the national security and the foreign policy of the United States.

NEWSLETTER NOTES

CrowdStrike update causes major IT outage, taking out banks, airlines and businesses across the world

Manish Singh
12:40 AM PDT • July 19, 2024

Businesses across the world are reporting IT outages, including Windows "blue screen of death" errors on their computers, in what has already become one of the most widespread IT disruptions in recent years. The outage — linked to an update rolled out for widely used security software made by cybersecurity firm CrowdStrike early on Friday — has affected computers running Microsoft Windows at companies across various sectors, from airlines, banks, food chains and brokerage houses, to news organizations, and railway networks. The travel sector seems to be the hardest hit.

CrowdStrike's chief executive, George Kurtz, confirmed that a 'defect' in a content update for Windows hosts had caused the outage, noting that Mac and Linux hosts were not impacted. He said the firm had identified, isolated and rolled out a fix.

****

Sanctioning Members of the Cyber Army of Russia Reborn

07/19/2024 10:55 AM EDT

Matthew Miller, Department Spokesperson
The United States is designating two members of the Russian hacktivist group Cyber Army of Russia Reborn (CARR) for their roles in cyber operations against U.S. critical infrastructure entities.

Since 2022, CARR has conducted malicious cyber activities against Ukraine and governments that support Ukraine. In late 2023, CARR escalated its operations, claiming responsibility for compromising the industrial control systems of multiple U.S. and European critical infrastructure targets. CARR has since been responsible for a slew of malicious cyber activities against water supply, hydroelectric, wastewater, and energy facilities in the United States and Europe.

Russia continues to provide a safe haven to cybercriminals and enable their malicious cyber activities against the United States and its allies and partners. While CARR's lack of sophistication and victims' responses have thus far prevented any instances of major damage, unauthorized access to critical infrastructure systems poses an elevated risk of harm to the public and can result in devastating humanitarian consequences.

Today's action furthers our efforts to combat foreign malicious cyber activity and sends a clear message that this activity will not be tolerated. We will continue to disrupt cybercriminals who seek to undermine our critical infrastructure and that of our partners.

Today's targets consist of the group's leader and primary hacker. The Department of the Treasury is taking these actions pursuant to Executive Order 13694 , as amended. For more information on this designation, see Treasury's press release .

Treasury Sanctions Rebel Alliance Driving Instability in the Democratic Republic of the Congo

July 25, 2024
United States targets armed group leaders who fuel conflict, displacement

WASHINGTON — Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) imposed sanctions on the Congo River Alliance, known by its French name *Alliance Fleuve Congo* (AFC), a coalition of rebel groups that seeks to overthrow the government of the Democratic Republic of Congo (DRC) and is driving political instability, violent conflict, and civilian displacement. The principal member of AFC is the U.S.- and UN-sanctioned March 23 Movement (M23), an armed group with a long history of destabilizing the DRC's North Kivu province and perpetrating human rights abuses. OFAC is also targeting individuals and entities associated with AFC, including Bertrand Bisimwa, the president of M23; Twirwaneho, an AFC-affiliated armed group in the DRC's South Kivu province; and Charles Sematama, a commander and deputy military leader of Twirwaneho.

"Today's action reinforces our commitment to hold accountable those who seek to perpetuate instability, violence, and harm to civilians to achieve their political goals," said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. "We condemn AFC and its affiliates, including M23, for fueling this deadly conflict and exacerbating a humanitarian crisis in eastern DRC."

In addition, OFAC is redesignating Corneille Yobeluo Nangaa (Nangaa), who launched AFC alongside the leaders of M23. Nangaa is the former president of the DRC's National Independent Electoral Commission (CENI) and was originally sanctioned by OFAC in 2019 for engaging in actions or policies that undermine democratic processes or institutions in the DRC. Today, he is also being sanctioned for acting as a leader of AFC. The designation of AFC and its affiliates and the redesignation of Nangaa are being carried out pursuant to Executive Order (E.O.) 13413, as amended by E.O. 13671.

CONGO RIVER ALLIANCE: A Driver of Political INSTABILITY IN Eastern DRC

The **Congo River Alliance (*Alliance Fleuve Congo* (AFC))** is a political-military coalition that seeks to overthrow the DRC government. At its launch on December 15, 2023, AFC invited armed groups and members of the Congolese military to join its rebellion. AFC conducts advocacy and public outreach on behalf of M23 and seeks to extend its armed insurgency beyond eastern DRC. AFC is being designated pursuant to E.O. 13413, as amended by E.O. 13671 ("E.O. 13413, as amended"), for having acted or purported to act for or on behalf of M23.

Corneille Yobeluo Nangaa (Nangaa) is the former president of CENI and was a key figure in the delay of the DRC's 2016 elections, which were postponed until 2018. Nangaa is the coordinator of AFC, which he launched alongside senior M23 officers. Nangaa is engaging in efforts to popularize AFC and promote its goal of overthrowing the DRC government, in collaboration with M23. OFAC designated Nangaa on March 21, 2019, pursuant to E.O. 13413, as amended, for engaging in actions or policies that undermine democratic processes or institutions in the DRC. Today, OFAC is also designating Nangaa pursuant to E.O. 13413, as amended, for being a leader of AFC.

(*Continued On The Following Page)

m23: A Rebellion at the center of recurring Violence in North Kivu

AFC's primary member is M23, a Rwanda-backed rebel group that seized vast swathes of eastern DRC in 2012 and briefly controlled the border city of Goma, before fleeing to neighboring Rwanda and Uganda in 2013. OFAC designated M23 on January 3, 2013, pursuant to E.O. 13413, for committing serious violations of international law involving the targeting of children in situations of armed conflict in the DRC, including killing and maiming, sexual violence, abduction, and forced displacement, and receiving arms and related materiel, including military aircraft and equipment, or advice, training, or assistance, including financing and financial assistance, related to military activities in the DRC.

M23 reemerged in late 2021 with the help of the Rwanda Defence Force (RDF). In February 2024, M23 cut off the last remaining overland supply route to Goma, and in May 2024, M23 seized Rubaya, a town at the center of an expansive mining area for coltan, a key material used in the production of electronic devices. The security crisis prompted by M23's rebellion has displaced around 1.5 million people according to the International Organization for Migration. Over the course of its rebellion, M23 has perpetrated human rights abuses, including killings, attacks against civilians, and sexual violence. On November 29, 2022, M23 conducted a series of killings in the town of Kishishe in North Kivu, where M23 combatants looted civilian property and raped women. Promoting accountability for conflict-related sexual violence committed by groups such as M23 is a top priority for President Biden, who signed a Presidential Memorandum on November 28, 2022 that directs the U.S. government to strengthen the exercise of its financial, diplomatic, and legal tools to address this pernicious problem.

Bertrand Bisimwa (Bisimwa) is the civilian president of M23. He stood alongside Nangaa at the launch of AFC and is central to AFC and M23's collaboration. Bisimwa engages in public outreach on behalf of M23 and facilitates the establishment of rebel administrations in territories controlled by M23. Bisimwa is being designated pursuant to E.O. 13413, as amended, for being a leader of M23.

Twirwaneho: Extending AFC's Rebellion TO South Kivu

Twirwaneho is an armed group in South Kivu province that is a member of AFC and collaborates with M23. The leader of Twirwaneho is Michel Rukunda (Rukunda), who was sanctioned by OFAC, along with other Congolese armed group leaders, on December 8, 2023 pursuant to E.O. 13413, as amended. In February 2024, the UN Security Council's 1533 DRC Sanctions Committee also added Rukunda to its sanctions list. Twirwaneho is responsible for attacks against civilians and forced recruitment, including of minors.

(*Continued On The Following Column)

Twirwaneho is being designated pursuant to E.O. 13413, as amended, for being responsible for or complicit in, or having engaged in, directly or indirectly, the targeting of women, children, or any civilians through the commission of acts of violence (including killing, maiming, torture, or rape or other sexual violence), abduction, forced displacement, or attacks on schools, hospitals, religious sites, or locations where civilians are seeking refuge, or through conduct that would constitute a serious abuse or violation of human rights or a violation of international humanitarian law in or in relation to the DRC.

Charles Sematama (Sematama) is a commander and deputy military leader of Twirwaneho. Sematama deserted from the Congolese military in February 2021 and leads Twirwaneho operations, including the armed group's forcible recruitment of minors. Sematama is being designated pursuant to E.O. 13413, as amended, for being a leader of Twirwaneho.

sANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the designated persons described above that are in the United States or in the possession or control of U.S. persons are blocked and must be reported to OFAC. In addition, any entities that are owned, directly or indirectly, individually or in the aggregate, 50 percent or more by one or more blocked persons are also blocked. Unless authorized by a general or specific license issued by OFAC, or exempt, OFAC's regulations generally prohibit all transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of designated or otherwise blocked persons.
In addition, the prohibitions include the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any designated person, or the receipt of any contribution or provision of funds, goods, or services from any such person.
The power and integrity of OFAC sanctions derive not only from OFAC's ability to designate and add persons to the SDN List, but also from its willingness to remove persons from the SDN List consistent with the law. The ultimate goal of sanctions is not to punish, but to bring about a positive change in behavior.

****

U.S. DEPARTMENT OF THE TREASURY
OFFICE OF FOREIGN ASSETS CONTROL

Enforcement Release: July 26, 2024
State Street Bank and Trust Company Settles with OFAC for $7,452,501 Related to Apparent Violations of the Ukraine-/Russia-Related Sanctions Regulations State Street Bank and Trust Company (State Street), a Massachusetts-based financial institution, on behalf of itself and its subsidiary, Charles River Systems, Inc. (Charles River), a Massachusetts-based non-bank technology company acquired by State Street in 2018, has agreed to pay $7,452,501 to settle their potential civil liability for apparent violations of OFAC's Ukraine-/Russia-Related Sanctions Regulations (URRSR). The apparent violations involved invoices that were redated or reissued by Charles River for certain customers who were subject to Directive 1 of Executive Order (E.O.) 13662, as well as certain payments accepted by Charles River from these customers. The 38 apparent violations occurred between 2016 and 2020, and involved invoices totaling approximately $1,270,456.

(*Continued on the Following Page)

The settlement amount reflects OFAC's determination that the apparent violations were egregious and not voluntarily self-disclosed. It also takes into account State Street's cooperation with OFAC's investigation (including its proactive notification to OFAC of its internal findings), and the remedial measures implemented by State Street upon discovery of the apparent violations.

Settlement Background

Directive 1 under E.O. 13662 is a "less-than-blocking" measure that prohibits U.S. persons from certain dealings in new debt of entities identified under the directive, beyond certain specified periods of maturity. Specifically, Directive 1 prohibits, among other things, all transactions in, provision of financing for, and other dealings in new debt of longer than 90, 30, or 14 days maturity (or "tenor") for such entities, depending on when the debt was issued.1 As relevant here, dealings in new debt of longer than 30 days maturity are prohibited for debt issued on or after September 12, 2014 and before November 28, 2017. Dealings in new debt of longer than 14 days maturity are prohibited for debt issued after November 28, 2017.

1 See Directive 1 (as most recently amended on September 29, 2017) under E.O. 13662. Directive 1 was initially issued on July 16, 2014, and prohibited U.S. persons from transacting in, providing financing for, or otherwise dealing in new debt of longer than 90 days maturity (among other prohibitions). Directive 1 was amended on September 12, 2014 to prohibit transacting in, providing financing for, or otherwise dealing in new debt of longer than 30 days maturity. On September 29, 2017, in accordance with the Countering Russian Influence in Europe and Eurasia Act of 2017 (CRIEEA) (see Title II of the Countering America's Adversaries Through Sanctions Act), Directive 1 was again amended (with a delayed effective date of November 28, 2017) to prohibit transacting in, providing financing for, or otherwise dealing in new debt of longer than 14 days maturity.

Persons identified by OFAC under Directive

1 are included on OFAC's Sectoral Sanctions Identifications (SSI) List.

2 Directive 1 applies to entities owned 50 percent or more by one or more persons identified under the directive.

3 Charles River's SSI Customers Between approximately 2008 and 2022, Charles River initiated and maintained various business relationships with subsidiaries owned 50 percent or more by Sberbank or VTB Bank. Both Sberbank and VTB Bank are Russian financial institutions that OFAC listed under Directive 1 in 2014, and whose majority-owned subsidiaries (the "SSI customers") are also subject to the Directive 1 prohibitions.

4 As part of its relationships with these entities, Charles River sold continuous access to a proprietary "point-to-point" communications network (the "FIX Network") that allowed customers to privately exchange trade information with their brokers. To utilize the network, each SSI customer signed its own master contract with Charles River that established general service and invoicing terms related to access and usage; subsequently, Charles River would bill the SSI customers through invoices issued pursuant to each customer's contract. For purposes of Directive 1, the issuance of an invoice represents a dealing in debt.

(*Continued on the Following Column)

Accordingly, payment on an invoice involving an SSI entity must be made within the applicable 90, 30, or 14-day limit imposed by Directive 1, depending upon the time period in which the invoice was issued. As a U.S. person, Charles River was prohibited from accepting payments from SSI customers outside the applicable debt tenor of a given invoice. Under Directive 1, U.S. persons are required to reject invoice payments beyond the applicable 90, 30, or 14-day limit.

Description of the Apparent Violations Between 2014 and 2020, Charles River received invoice payments from its SSI customers through at least one U.S. financial institution. As early as 2014, Charles River was aware that payments were being scrutinized and delayed by the U.S. financial institution due to U.S. sanctions. During its reviews of payments subject to Directive 1, the U.S. financial institution requested copies of related payment documentation from Charles River, including applicable invoices and underlying customer contracts.

The most recent version of the Sectoral Sanctions Identifications List is available on OFAC's Additional Sanctions

See OFAC Frequently Asked Question 373.

See Federal Register Notice, Sanctions Actions Pursuant to Executive Orders 13660, 13661 and 13662, 79 Fed. Reg 63021-29 (Oct. 21, 2014).

In addition to being subject to Directive 1 under E.O. 13662, VTB and Sberbank are also subject to other OFAC sanctions that are not at issue in this case. On February 24, 2022, VTB Bank was identified as a blocked person under E.O. 14024 and Sberbank was identified as an entity subject to Directive 1 under E.O. 14024, "Prohibitions Related to Correspondent or Payable-Through Accounts and Processing of Transactions Involving Certain Foreign Financial Institutions" (the "Russia-related CAPTA Directive"). On April 6, 2022, Sberbank also was identified as a blocked person under E.O. 10424. Both VTB Bank and Sberbank remain listed as entities subject to Directive 1 under E.O. 13662.

See OFAC Frequently Asked Question 419.

See OFAC Frequently Asked Question 370.

By at least 2016, two years before State Street acquired Charles River, the abovementioned U.S. financial institution had rejected two payments that were remitted by SSI customers outside of applicable debt tenors based on Charles River's invoice dates. Correspondence indicates that Charles River reached out directly to these SSI customers to inquire about their failure to pay outstanding invoices. Citing what it described as "sanctions difficulties," at least one SSI customer asked Charles River to redate invoices that were more than 30 days old (the applicable debt tenor at the time) to prevent associated payments from being rejected when they reached correspondent and beneficiary financial institutions in the United States.

Following internal deliberation and requests from its SSI customers, Charles River staff began regularly redating or reissuing "old" invoices—redating at least one invoice as many as six times—which disguised their original dates of issuance and made them appear more recent. As a collections manager stated on one occasion, she would, "do whatever it takes to get this invoice paid." Ostensibly "new" invoices were manually created by Charles River, which kept records of the original invoices and dates in its internal systems and then submitted the altered invoices to at least one U.S. financial institution to prevent it from rejecting late payments from SSI customers under the then-applicable tenor. Throughout this time, Charles River also accepted multiple late payments from SSI customers that occurred outside of the payment windows established by directive 1.

(*Continued On The Following Page)

At least 18 staff members from multiple internal offices (including accounting, collections, and client management) were involved in, or aware of, the reissuance or redating of invoices for SSI entities. Despite its status as a mid-sized company that provided finance-related technology services to clients in more than 30 countries, Charles River maintained minimal compliance procedures prior to its 2018 acquisition by State Street. Charles River staff demonstrated a varying, but limited, understanding of Charles River's sanctions-related obligations (including Directive 1), and engaged in a pattern of disregarding the sanctions implications of payment rejections during this time period, despite receiving general sanctions-related payment guidance from the company's U.S. financial institution.

Indeed, on multiple occasions, the U.S. financial institution that routinely rejected late SSI customer payments provided Charles River with a guidance document for customers engaged in sanctions-related transactions, including Ukraine/Russia-related payments. In at least one instance, the financial institution provided Charles River with a second guidance document concerning economic sanctions policies and enforcement, as well as the financial institution's sanctions obligations and internal controls. The guidance noted that the financial institution's status as a U.S. company required it to comply with OFAC sanctions laws and advised that attempts to evade a bank's controls (including the manipulation of information related to a transaction) could be considered a serious offense by government authorities. The financial institution further advised Charles River to seek additional information about E.O. 13662 from government-published sources.

The apparently violative activity addressed in this settlement occurred over the course of at least four years between December 2016 and May 2020, including 19 months following Charles River's acquisition by State Street in October 2018. Although State Street performed a post-acquisition onboarding analysis in which it correctly identified certain Charles River clients as entities that were subject to Directive 1, this analysis did not consider the Directive's applicability to late invoice payments; subsequent screening alerts concerning payments from SSI customers were manually dismissed without accounting for these restrictions.

As a result of the conduct described above, Charles River appears to have violated E.O. 13662 by engaging in activities that it should have known violated or were likely to violate U.S. sanctions. This conduct resulted in 38 apparent violations of the URRSR, 31 C.F.R. § 589.202 (the "Apparent Violations") that occurred when Charles River staff either redated and reissued invoices or accepted invoice payments after the expiration of an applicable Directive 1 debt tenor. The Settlement Agreement for this action can be found here.

Penalty Calculations and General Factors Analysis

The statutory maximum civil monetary penalty applicable in this matter is $13,550,002. OFAC determined that neither State Street nor Charles River voluntarily self-disclosed the Apparent Violations and that the Apparent Violations constitute an egregious case. Accordingly, under OFAC's Economic Sanctions Enforcement Guidelines ("Enforcement Guidelines"), 31 C.F.R. Part 501, app. A, the base civil monetary penalty applicable in this matter equals the statutory maximum, which is $13,550,002.

(*Continued On The Following Column)

The settlement amount of $7,452,501 reflects OFAC's consideration of the General Factors under the Enforcement Guidelines. OFAC determined the following to be aggravating factors:

(1) Charles River appeared to at least recklessly violate Directive 1 of E.O. 13662 on 38 occasions by reissuing or redating invoices and accepting invoice payments outside of applicable Directive 1 debt tenors over the course of four years, despite being aware as early as 2014 that certain customer payments were subject to sanctions-related limitations. In doing so, Charles River failed to institute or conduct internal compliance procedures to address the risks posed by its relationships with its clients. Instead, Charles River staff sought payments for previously rendered services by reissuing and redating invoices and submitting them to at least one U.S. financial institution to prevent it from rejecting late payments from SSI customers under the then-applicable tenor.

(2) Charles River's apparently violative activity continued despite multiple rejection notices from a U.S. financial institution that referenced E.O. 13662, and both U.S. sanctions authorities generally and OFAC specifically. The financial institution also provided Charles
River with follow-up guidance for sanctions-related payments, and instructed Charles River to seek additional related information from the U.S. government.

(3) At least 18 Charles River staff members from multiple internal offices (including accounting, collections, and client management) were involved in, or aware of, the reissuance or redating of invoices for SSI customers. Charles River's activity also continued for 19 months after its acquisition by State Street in 2018, during which Charles River's customers were onboarded and integrated into State Street's existing compliance program.

Throughout this post-acquisition period, State Street's staff dismissed multiple automatic screening alerts concerning payments from Charles River's SSI customers without considering the application of Directive 1 to the activity at issue.

Charles River is a commercially sophisticated company that employed more than 750 people and served clients in more than 30 countries at the time of the apparently violative activity.

Although Charles River is a non-bank entity, its provision of investment-related technology services to banking entities indicated an institutional familiarity with the financial sector.
State Street is a large and sophisticated global financial institution.
OFAC determined the following to be mitigating factors:
(1) Neither State Street nor Charles River has received a penalty notice from OFAC in the five years preceding the earliest date of the transactions giving rise to the Apparent Violations.
(2) State Street implemented remedial measures to its compliance program following an internal investigation into Charles River's conduct, including: (i) amendments to its global sanctions policies; (ii) onboarding prohibitions for all Directive 1 and Directive 1-owned entities; (iii) updates to its alert disposition processes; (iv) training for certain Charles River staff members; and (v) increased monitoring of sanctions issues within State Street management. State Street ultimately terminated all relationships with SSI entities (including Directive 1 entities) that were previously Charles River clients by February 2022. State Street also increased the size of its sanctions compliance review team by 25 percent in 2022.
(3) Although OFAC had previously received reject reports from Charles River's U.S. financial institution, State Street fulsomely reported on the matter to OFAC and during the investigation by disclosing additional apparent violations, submitting detailed documentation, responding quickly and fully to OFAC's requests, and entering into tolling agreements.

(*Continued on the Following Page)

Compliance Considerations

This enforcement action highlights the importance of establishing and maintaining effective sanctions compliance policies, procedures, and controls that are commensurate with a company's business operations and customer base. In addition to accounting for blocking, jurisdictional, and other standard prohibitions, these policies should be sure to convey the importance of and institute controls for examining clients and activities that may be subject to "less-than-blocking" sectoral sanctions, including debt- and equity-related limitations. Such comprehensive compliance policies and training can also help foster an internal culture of compliance to assist staff in effectively responding to warning signs regarding potential violations, including transactions that have been 7 A Finding of Violation issued to State Street on April 30, 2019 was not substantially similar to the subject case, as it addressed violations related to pension payments processed by State Street to the U.S. bank account of a resident of Iran blocked or rejected by their financial institutions in accordance with OFAC regulations. Companies should further consider any compliance needs that may arise when new clients are onboarded following mergers or acquisitions. Even after onboarding is complete, companies should closely monitor their new business relationships for sanctions-related issues that may require preventative or remedial measures.

Companies should also be prepared to adequately address scenarios where the activities of certain customers (including entities subject to sectoral sanctions) may trigger internal compliance concerns. Such scenarios could include instances where counterparties routinely fail to pay invoices within applicable payment windows, resulting in the rejection of payments by U.S. financial institutions. As noted in OFAC Frequently Asked Question 419, if a U.S. person believes that it may not receive payment in full by the end of the relevant payment period, the U.S. person should contact OFAC.8 Companies should also exercise extreme caution if entities subject to sectoral sanctions ask U.S. parties to engage in deceptive or unorthodox business practices, particularly those involving accounting and recordkeeping standards. Companies should never falsify payment-related supporting documentation to facilitate the processing of transactions that would otherwise be prohibited by U.S. sanctions.

Finally, this enforcement action further emphasizes the importance of understanding and adhering to the prohibitions set forth in OFAC's sectoral sanctions programs. Sectoral sanctions are an important element of OFAC's foreign policy and national security goals, and OFAC is committed to enforcing against these programs. Companies that onboard or otherwise do business with non-blocked entities that are subject to sectoral sanctions, including entities owned more than 50 percent by SSI entities under E.O. 13662, must ensure that they comply with all aspects of these sanctions.

OFAC Enforcement and Compliance Resources

On May 2, 2019, OFAC published A Framework for OFAC Compliance Commitments (Framework) in order to provide organizations subject to U.S. jurisdiction, as well as foreign entities that conduct business in or with the United States or U.S. persons, or that use goods or services exported from the United States, with OFAC's perspective on the essential components of a sanctions compliance program. The Framework also outlines how OFAC may incorporate these components into its evaluation of apparent violations and resolution of investigations resulting in settlements. The Framework includes an appendix that offers a brief analysis of some of the root causes of apparent violations of U.S. economic and trade sanctions programs OFAC has identified during its investigative process.

(*Continued On The Following Column)

Information concerning the civil penalties process can be found in the OFAC regulations governing each sanctions program; the Reporting, Procedures, and Penalties Regulations, 31 C.F.R. part 501; and the Enforcement Guidelines. These references, as well as recent civil penalties and enforcement information, can be found on OFAC's website at https://ofac.treasury.gov/civil-penalties-and-enforcement-information. See OFAC Frequently Asked Question 419.

Whistleblower Program

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) maintains a whistleblower incentive program for violations of OFAC-administered sanctions, in addition to violations of the Bank Secrecy Act. Individuals located in the United States or abroad who provide information may be eligible for awards, if the information they provide leads to a successful enforcement action that results in monetary penalties exceeding $1,000,000. FinCEN is currently accepting whistleblower tips.

For more information regarding OFAC regulations, please go to: https://ofac.treasury.gov/.

****

FOR IMMEDIATE RELEASE - Friday, July 26, 2024
AI GUIDANCE LINK FOUND AT BOTTOM OF ARTICLE

Media Contact: Office of Public Affairs, publicaffairs@doc.gov

Department of Commerce Announces New Guidance, Tools 270 Days Following President Biden's Executive Order on AI ***For the first time, Commerce makes public new NIST draft guidance from U.S. AI Safety Institute to help AI developers evaluate and mitigate risks stemming from generative AI and dual-use foundation models.**Read the White House Fact sheet on Administration-wide actions on AI.*

The U.S. Department of Commerce announced today, on the 270-day mark since President Biden's Executive Order (EO) on the Safe, Secure and Trustworthy Development of AI, the release of new guidance and software to help improve the safety, security and trustworthiness of artificial intelligence (AI) systems.

The Department's National Institute of Standards and Technology (NIST) released three final guidance documents that were first released in April for public comment, as well as a draft guidance document from the U.S. AI Safety Institute that is intended to help mitigate risks. NIST is also releasing a software package designed to measure how adversarial attacks can degrade the performance of an AI system. In addition, Commerce's U.S. Patent and Trademark Office (USPTO) issued a guidance update on patent subject matter eligibility to address innovation in critical and emerging technologies, including AI,"Under President Biden and Vice President Harris' leadership, we at the Commerce Department have been working tirelessly to implement the historic Executive Order on AI and have made significant progress in the nine months since we were tasked with these critical responsibilities," said U.S. Secretary of Commerce Gina Raimondo. "AI is the defining technology of our generation, so we are running fast to keep pace and help ensure the safe development and deployment of AI. Today's announcements demonstrate our commitment to giving AI developers, deployers, and users the tools they need to safely harness the potential of AI, while minimizing its associated risks. We've made great progress, but have a lot of work ahead. We will keep up the momentum to safeguard America's role as the global leader in AI."

(*Continued On The Following Page)

NIST's document releases cover varied aspects of AI technology. Two were made public today for the first time. One is the initial public draft of a guidance document from the U.S. AI Safety Institute, and is intended to help AI developers evaluate and mitigate the risks stemming from generative AI and dual-use foundation models — AI systems that can be used for either beneficial or harmful purposes. The other is a testing platform designed to help AI system users and developers measure how certain types of attacks can degrade the performance of an AI system. Of the remaining three document releases, two are guidance documents designed to help manage the risks of generative AI — the technology that enables many chatbots as well as text-based image and video creation tools — and serve as companion resources to NIST's AI Risk Management Framework (AI RMF) and Secure Software Development Framework (SSDF). The third proposes a plan for U.S. stakeholders to work with others around the globe on AI standards.

"For all its potentially transformational benefits, generative AI also brings risks that are significantly different from those we see with traditional software," **said Under Secretary of Commerce for Standards and Technology and NIST Director Laurie E. Locascio**. "These guidance documents and testing platform will inform software creators about these unique risks and help them develop ways to mitigate those risks while supporting innovation."

USPTO's guidance update will assist USPTO personnel and stakeholders in determining subject matter eligibility under patent law (35 U.S.C. § 101) of AI inventions. This latest update builds on previous guidance by providing further clarity and consistency to how the USPTO and applicants should evaluate subject matter eligibility of claims in patent applications and patents involving inventions related to AI technology. The guidance update also announces three new examples of how to apply this guidance throughout a wide range of technologies.

"The USPTO remains committed to fostering and protecting innovation in critical and emerging technologies, including AI," **said Kathi Vidal, Under Secretary of Commerce for Intellectual Property and Director of the USPTO**. "We look forward to hearing public feedback on this guidance update, which will provide further clarity on evaluating subject matter eligibility of AI inventions while incentivizing innovations needed to solve world and community problems."

NTIA's soon-to-be-published report will review the risks and benefits of dual-use foundation models whose model weights are widely available (i.e. "open-weight models"), as well as develop policy recommendations maximizing those benefits while mitigating the risks. Open-weight models allow developers to build upon and adapt previous work, broadening AI tools' availability to small companies, researchers, nonprofits, and individuals.

Additional information on today's announcements from NIST can be found below.

Protecting Against Misuse Risk from Dual-Use Foundation Models

AI foundation models are powerful tools that are useful across a broad range of tasks and are sometimes called "dual-use" because of their potential for both benefit and harm. NIST's U.S. AI Safety Institute has released the initial public draft of its guidelines on *Managing Misuse Risk for Dual-Use Foundation Models*, which outlines voluntary best practices for how foundation model developers can protect their systems from being misused to cause deliberate harm to individuals, public safety and national security.

(*Continued On The Following Column)

The draft guidance offers seven key approaches for mitigating the risks that models will be misused, along with recommendations for how to implement them and how to be transparent about their implementation. Together, these practices can help prevent models from enabling harm through activities like developing biological weapons, carrying out offensive cyber operations, and generating child sexual abuse material and non-consensual intimate imagery.

The AI Safety Institute is accepting comments from the public on the draft *Managing the Misuse Risk for Dual-Use Foundation Models* until [DATE]. Comments can be submitted electronically to NISTAI800-1@nist.gov with "NIST AI 800-1, Managing Misuse Risk for Dual-Use Foundation Models" in the subject line.

Testing how AI Models Respond to Attacks

One of the vulnerabilities of an AI system is the model at its core. By exposing a model to large amounts of training data, it learns to make decisions. But if adversaries poison the training data with inaccuracies — for example, by introducing data that can cause the model to misidentify stop signs as speed limit signs — the model can make incorrect, potentially disastrous decisions. Testing the effects of adversarial attacks on machine learning models is one of the goals of Dioptra, a new software package aimed at helping AI developers and customers determine how well their AI software stands up to a variety of adversarial attacks.

The open-source software, available for free download, could help the community including government agencies and small- to medium-sized businesses conduct evaluations to assess AI developers' claims about their systems' performance. This software responds to Executive Order section 4.1 (ii) (B), which requires NIST to help with model testing. Dioptra does this by allowing a user to determine what sorts of attacks would make the model perform less effectively and quantifying the performance reduction so that the user can learn how often and under what circumstances the system would fail.

Managing the Risks of Generative AI

The *AI RMF Generative AI Profile* (NIST AI 600-1) can help organizations identify unique risks posed by generative AI and proposes actions for generative AI risk management that best aligns with their goals and priorities. The guidance is intended to be a companion resource for users of NIST's AI RMF. It centers on a list of 12 risks and just over 200 actions that developers can take to manage them. The 12 risks include a lowered barrier to entry for cybersecurity attacks, the production of mis- and disinformation or hate speech and other harmful content, and generative AI systems confabulating or "hallucinating" output. After describing each risk, the document presents a matrix of actions that developers can take to mitigate them, mapped to the AI RMF.

Reducing Threats to the Data Used to Train AI Systems

The second finalized publication, *Secure Software Development Practices for Generative AI and Dual-Use Foundation Models* (NIST Special Publication (SP) 800-218A), is designed to be used alongside the Secure Software Development Framework (SP 800-218). While the SSDF is broadly concerned with software coding practices, the companion resource expands the SSDF in part to address a major concern with generative AI systems: They can be compromised with malicious training data that adversely affect the AI system's performance.

(*Continued On The Following Page)

In addition to covering aspects of the training and use of AI systems, this guidance document identifies potential risk factors and strategies to address them. Among other recommendations, it suggests analyzing training data for signs of poisoning, bias, homogeneity and tampering.

Global Engagement on AI Standards

AI systems are transforming society not only within the U.S., but around the world. *A Plan for Global Engagement on AI Standards* (NIST AI 100-5), today's third finalized publication, is designed to drive the worldwide development and implementation of AI-related consensus standards, cooperation and coordination, and information sharing.

The guidance is informed by priorities outlined in the NIST-developed Plan for Federal Engagement in AI Standards and Related Tools and is tied to the National Standards Strategy for Critical and Emerging Technology. This publication suggests that a broader range of multidisciplinary stakeholders from many countries participate in the standards development process.

GUIDANCE LINK:

https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.800-1.ipd.pdf

https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf

https://www.nist.gov/standardsgov/usg-nss

****

Will S. Korea join AUKUS Pillar 2 in face of deepening Russia-NK ties?

Updated : 2024-07-15 10:34

Experts fear Seoul's participation can further strain relations with Beijing - By Kwak Yeon-soo

There is an ongoing discussion as to whether South Korea will join the AUKUS Pillar 2 in the face of deepening military cooperation between North Korea and Russia.

The AUKUS — an acronym for Australia, the U.K. and the U.S. — is a trilateral security partnership formed among the three countries in 2021 to counter China's growing influence in the Indo-Pacific region. Pillar 2 of the AUKUS aims to share advanced military technology in areas such as hypersonic missiles, artificial intelligence and cyber technology, whereas Pillar 1 involves delivering nuclear-powered submarines to Australia.

In May, Defense Minister Shin Won-sik said the possibility of joining the AUKUS Pillar 2 was discussed during a "2 Plus 2" meeting among foreign and defense ministers in Melbourne, Australia.

"We do welcome that AUKUS members are considering South Korea as an AUKUS Pillar 2 partner. Korea's defense science and technology capabilities will contribute to the peace and stability of the development of the AUKUS Pillar 2 and regional peace," Shin said during a press conference following the meeting.

(*Continued On The Following Column)

Last month's summit between Russian President Vladimir Putin and North Korean leader Kim Jong-un strengthened military alliance between the two countries, putting South Korea's security at risk. The two signed a comprehensive strategic partnership agreement, which involves providing mutual defense assistance in case either side faces an armed attack.

The government is now facing growing calls to engage in discussions with AUKUS members to weigh up the economic and security benefits and costs about whether joining Pillar 2 is in the national interest. The presidential office said it is in the early stages of discussion and it would require a considerable amount of time for review.

Although nothing has been decided yet, experts see Seoul's participation as an opportunity to boost deterrence against North Korea and other security threats.

"South Korea has much to gain from joining AUKUS Pillar 2, especially around this time when North Korea and Russia are strengthening military ties," Ban Kil-joo, a research professor at Korea University, said. "The AUKUS Pillar 2 isn't just a security partnership. It's more like a new Cold War-era military alliance. Thus, it will contribute to peace and stability in the region."

Doo Jin-ho, a research fellow at the Center for Security and Strategy in the Korea Institute for Defense Analyses, said joining AUKUS Pillar 2 would mean falling under U.S.-led "lattice-like architecture." This strategic framework refers to several small cooperation groups, including South Korea-U.S.-Japan trilateral cooperation, the AUKUS and the Quad.

"If South Korea joins the AUKUS Pillar 2, it will be able to deter, defend and respond to threats from North Korea, among other regional threats. The U.S., U.K. and Australia will provide security assurance and South Korea will be able to learn about emerging military technologies,"

However, experts pointed out that joining the AUKUS Pillar 2 would also come with risks.

Seoul's participation would likely deteriorate its already-tense relationship with Beijing, since the pact is widely seen as part of U.S.-led efforts to counter China's assertiveness in the region.

The Chinese Embassy in Washington objected to the arrangement, saying "AUKUS is essentially about fueling military confrontation through military collaboration."

"It (AUKUS) creates additional nuclear proliferation risks, exacerbates the arms race in the Asia-Pacific and hurts regional peace and stability. China is deeply concerned and firmly opposed to it," Liu Pengyu, a spokesperson for the Chinese Embassy in Washington, told VOA on May 6.

Ban said, "China will probably be upset if South Korea participates in AUKUS Pillar 2, but I think we should manage the risk by assuring China that Pillar 2 is a platform for technology collaboration."

(*Continued On The Following Page)

Doo feared that the government's efforts to stabilize ties with China might come to nothing. South Korean and Chinese foreign ministers resumed talks and Seoul hosted a long-suspended South Korea-Japan-China trilateral summit in May.

"Seoul will likely face a strong opposition from Beijing. China may retaliate by joining forces with North Korea and Russia, heightening tensions on the Korean Peninsula," Doo said.

Pundits suggested South Korea should adopt strategic ambiguity until the U.S. election.

"There is no need to make a hasty decision. We can use it as a leverage tool to engage with like-minded countries and deter North Korean aggression," Doo said.

Meanwhile, Japan, New Zealand and Canada are reportedly under consideration for AUKUS Pillar 2 partners.

****

Alabama Man Pleads Guilty to Violating Iran Sanctions

Thursday, July 18, 2024

Ray Hunt, also known as Abdolrahman Hantoosh, Rahman Hantoosh and Rahman Natooshas, 70, of Owens Cross Roads, Alabama, pleaded guilty today to conspiracy to export U.S.-origin goods to the Islamic Republic of Iran in violation of trade sanctions.

According to court documents, in May 2014, Hunt registered Vega Tools LLC with the Alabama Secretary of State, listing the nature of the business as "the purchase/resale of equipment for the energy sector." He operated Vega Tools, including purchasing, receiving and shipping U.S.-origin goods, from locations in Madison County, Alabama. Beginning at least as early as 2015, Hunt conspired with two Iranian companies located in Tehran, Iran, to illegally export U.S.-manufactured industrial equipment for use in Iran's oil, gas and petrochemical industries.

Hunt engaged in a series of deceptive practices to avoid detection by U.S. authorities, including using third-party transshipment companies in Turkey and the United Arab Emirates (UAE) and routing payments through UAE banks, as well as lying to shipping companies about the value of his exports to prevent the filing of electronic export information to U.S. authorities. Hunt lied to suppliers and shippers by claiming the items he purchased on behalf of the Iranian co-conspirators were destined for end users in Turkey and UAE, while knowing the exports were ultimately destined for Iran. Hunt lied also to U.S. Customs and Border Patrol officers regarding the nature and existence of his business when questioned upon his return from a March 2020 trip to Iran.

Hunt pleaded guilty to a conspiracy charge and faces a maximum penalty of five years in prison. A federal district court judge will determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors.

(*Continued On The Following Column)

Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division, U.S. Attorney Prim F. Escalona for the Northern District of Alabama, Assistant Secretary of Commerce for Export Enforcement Matthew S. Axelrod and Executive Assistant Director Robert Wells of the FBI National Security Branch made the announcement.

The Department of Commerce Bureau of Industry and Security is investigating the case with valuable assistance provided by the FBI. Assistant U.S. Attorneys Jonathan "Jack" Harrington, Jonathan Cross and Henry Cornelius for the Northern District of Alabama and Trial Attorneys Emma Ellenrieder and Adam Barry of the National Security Division's Counterintelligence and Export Control Section are prosecuting the case.

****

Iran FDP Media Advisory

Today, the Department of Commerce's Bureau of Industry and Security (BIS) is implementing an expansion of controls on the export, reexport, or transfer (in-country) of certain foreign-produced items located in or destined to Iran, to address ongoing concerns regarding Iran's potential use of U.S. technology in weapons systems.

This rule implements the requirements of the No Technology for Terror Act (the Act), which was passed in April as part of emergency supplemental appropriations for the current fiscal year. As required by the Act, the BIS rule expands the scope of the Export Administration Regulations' (EAR) Iran Foreign Direct Product rule (FDPR). The expansion, effective July 23, 2024, is designed to further impede Iran's ability to procure technology and components critical for military systems, including advanced drones that pose threats to U.S. forces and allies.

Today's expanded controls build upon existing restrictions on Iran that apply under the Iran FDPR by imposing licensing requirements for the export, reexport, and transfer (in-country) of additional foreign-produced items located in or destined to Iran and by adding a new end-user scope that targets transactions involving such items in which the Government of Iran is a party.
This rule reflects our efforts to ensure robust enforcement of export controls and to prevent the proliferation of weapons systems that threaten U.S. troops overseas or key allies.

****

FOR IMMEDIATE RELEASE

July 25, 2024
www.bis.gov

BUREAU OF INDUSTRY AND SECURITY
Office of Congressional and Public Affairs
OCPA@bis.doc.gov

Commerce Proposes Restrictions on U.S. Persons' Support for Foreign Military, Intelligence, and Security Services and Controls to Protect National Security and Human Rights

New Rules Implement Provision from Fiscal Year 2023 Defense Authorization Law

(*Continued On The Following Page)

WASHINGTON, D.C. – Today, the U.S. Commerce Department's Bureau of Industry and Security (BIS) published proposed rules seeking public comment on enhanced restrictions on exports, reexports, or support to military or intelligence end users and end uses in countries of concern, consistent with the Fiscal Year 2023 National Defense Authorization Act (NDAA). These rules complement proposed revisions, also published today, regarding the scope of defense services controlled by the Department of State's Directorate of Defense Trade Controls (DDTC) pursuant to the International Traffic in Arms Regulations (ITAR). We encourage public comment on today's proposed rules, which include expanding restrictions against exporting items to, or providing support for, military or intelligence services in countries of concern.

"We must prevent hack-for-hire business models from circumventing our human rights-based export controls, such as those on cyber-intrusion tools," **said Assistant Secretary of Commerce for Export Administration Thea D. Rozman Kendler**. "Today, we are proposing enhanced controls on activities supporting foreign police and security services, including those known to violate human rights, as well as new controls on facial recognition technologies that can enable mass surveillance."

The proposed BIS rules build on existing Export Administration Regulations (EAR) restrictions on U.S. persons'[1] implement a provision of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2023,[2] originally authored via an amendment by Senator Ron Wyden (D-OR)[3]. These rules propose to implement the broadest expansion of presidential export control authority since the Export Control Reform Act (ECRA) was signed in August 2018. Specifically, as expanded by the NDAA for FY 2023, ECRA provides BIS with the authority to impose controls on the activities of U.S. persons, wherever located, relating to foreign military services, foreign intelligence services, and foreign security services. In amending ECRA in this manner, Congress sought to prevent U.S. persons from assist in foreign military, intelligence, and security services that threaten international peace and stability or spy on dissidents, journalists, and American citizens.

The specific controls proposed in today's rules include:

- **U.S. Persons' Activity Controls:** Expanded restrictions on U.S. persons' support activities regarding end uses and end users of concern, including facilitating the acquisition of certain foreign-origin items by military, intelligence, and security services of concern, as well as performing maintenance, repair, and overhaul of such foreign-origin items.
- **End-Use and End-User Controls**Expanded restrictions to apply to all items subject to the EAR when destined to the armed forces or national guard of countries subjected to a U.S. arms embargo[4], as well as civilian or military intelligence agencies (*i.e.,* intelligence end users) of over 40 countries of concern. Such controls are also proposed to apply to all items on the Commerce Control List when destined to foreign-security end users (*e.g.,* police and security agencies) or military-support end users (e.g., defense contractors) in countries subject to a U.S. arms embargo.
- **Item Controls:** New restrictions on the export of certain facial recognition technologies that can enable mass surveillance to protect and promote human rights.

(*Continued On The Following Column)

The controls proposed today complement controls maintained by other federal agencies, including controls on defense articles and services administered by DDTC pursuant to the Arms Export Control Act and the ITAR, as well as restrictions on U.S. persons' services maintained by the Department of the Treasury's Office of Foreign Assets Control under various sanctions programs. Under the proposed rules, U.S. persons would not be required to obtain a license from BIS to engage in activities regulated by another federal department or agency or required in furtherance of defense services authorized by DDTC.

Additional Information:

The text of the proposed rules is available on the Federal Register's website HERE and HERE BIS is inviting public comments, which are due 60 days after publication. Stakeholders are encouraged to submit their feedback by the deadline to ensure that the final provisions reflect broad industry and public input. You may submit comments for the military, intelligence, and military support end user/use rule by identified docket number BIS-2024-0029 or RIN 0694-AJ43. For the foreign security end user rule, the identified docket number is BIS-2023-0006 or RIN 0694-AI35. All comments must be submitted through the Federal eRulemaking Portal: https://www.regulations.gov.

****

Sanctions on Houthi Procurement Network

07/31/2024 12:33 PM EDT

Matthew Miller, Department Spokesperson

Ansarallah, commonly referred to as the Houthis, relies on a global network of procurement operatives, facilitators, and suppliers to acquire and transport dual-use components and equipment needed to develop and deploy advanced weapons systems, which they use to threaten commercial shipping in the Red Sea and surrounding waterways. Today, the United States is sanctioning two individuals and four entities in connection to the procurement of weapons for the Iran-backed Houthis and the provision of military grade and dual-use equipment to the Houthis.

Houthi-affiliated shipping firms have enabled the group to transfer military-grade components from People's Republic of China (PRC)-based suppliers to Yemen. One of today's targets, Al-Shahari United Corporation Ltd., is a Yemen-based logistics company that has facilitated numerous shipments from PRC-based suppliers to the Houthis, including components for use in Houthi missiles and unmanned aerial vehicles.

Houthi attacks continue to disrupt the flow of international trade and freedom of navigation. The United States will not hesitate to use all the tools at our disposal to deny the Houthis the ability to carry out such attacks.

The Department of the Treasury's sanctions actions were taken pursuant to counterterrorism authority Executive Order 13224, as amended. For more information, see Treasury's press release.

Treasury Targets Houthi Weapons Procurement Networks

July 31, 2024

WASHINGTON — Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is sanctioning two individuals and four companies that have facilitated weapons procurement for Ansarallah, commonly referred to as the Houthis. Since November 2023, the Houthis have deployed a range of unmanned aerial vehicles (UAVs), ballistic missiles, and cruise missiles to attack U.S. military forces, merchant vessels, their crews, and civilian populations in Israel. To undertake their reckless campaign targeting U.S. and allied interests, the Houthis rely on a global network of procurement operatives, shipment facilitators, and suppliers to procure and transport dual-use components and equipment needed to manufacture and deploy a range of advanced weapons systems. This action targets key actors located in the People's Republic of China (PRC), including Hong Kong, and Yemen who have directly supported Houthis' efforts to procure military-grade materials abroad and ship these items to Houthi-controlled areas of Yemen, enabling the group's ongoing attacks.

"The Houthis have sought to exploit key jurisdictions like the PRC and Hong Kong in order to source and transport the components necessary for their deadly weapons systems," said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. "Treasury will continue to target the facilitators that enable the Houthis' destabilizing activities."

Today's action is being taken pursuant to the counterterrorism authority Executive Order (E.O.) 13224, as amended, and builds on OFAC's June 17, 2024 action targeting seven individuals and entities enabling Houthi weapons procurement. The U.S. Department of State designated Ansarallah as a Specially Designated Global Terrorist (SDGT) pursuant to E.O. 13224, as amended, effective February 16, 2024, for having committed or attempted to commit, posing a significant risk of committing, or having participated in training to commit acts of terrorism.

HOUTHI-LINKED TRANSSHIPMENT COMPANIES

Houthi-affiliated shipping firms have enabled the group to transfer military-grade components from PRC-based suppliers to Yemen. One such firm, **Al-Shahari United Corporation Ltd.** (Al-Shahari United), is a Sanaa, Yemen-based logistics company that has facilitated numerous shipments from PRC-based suppliers to the Houthis, including components for use in Houthi missile and UAV manufacturing. Al-Shahari United maintains close contact with Houthi operatives based in the PRC and Yemen, who have used the company to help facilitate some of their most important procurement efforts.

Al-Shahari United relies on its PRC-based branch, **Guangzhou Alshahari United Corporation Limited** (Guangzhou Alshahari), to help facilitate shipments from the PRC to Yemen. Guangzhou Alshahari is wholly owned by Hong Kong-based **Hongkong Alshahari United Corporation Limited** (Hongkong Alshahari). **Ahmed Khaled Yahya Al-Shahare** is the Director and General Manager of Guangzhou Alshahari.

(*Continued On The Following Column)

Al-Shahari United is being designated pursuant to E.O. 13224, as amended, for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, Ansarallah. Guangzhou Alshahari is being designated pursuant to E.O. 13224, as amended, for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, Al-Shahari United. Hongkong Alshahari is being designated pursuant to E.O. 13224, as amended, for owning or controlling Guangzhou Alshahari. Ahmed Khaled Yahya Al-Shahare is being designated pursuant to E.O. 13224, as amended, for being a leader or official of Guangzhou Alshahari.

HOUTHI PROCUREMENT OPERATIONS IN YEMEN

Maher Yahya Muhammad Mutahar al-Kinai (al-Kinai) is a Yemeni businessman who has supported Houthi military procurement and smuggling efforts. Al-Kinai has coordinated with other Houthi procurement operatives to facilitate shipments of dual-use equipment and components for likely use in Houthi weapons manufacturing. Al-Kinai is the General Manager of **Yemen Telecommunication Asset Company for Information Technology** (Y-TAC), a Sanaa, Yemen-based company that has supported Houthi weapons and component procurement efforts.

Al-Kinai and Y-TAC are being designated pursuant to E.O. 13224, as amended, for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, Ansarallah.

SANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the individuals named above, and of any entities that are owned, directly or indirectly, 50 percent or more by them, individually, or with other blocked persons, that are in the United States or in the possession or control of U.S. persons must be blocked and reported to OFAC. OFAC's regulations generally prohibit all dealings by U.S. persons or within the United States (including transactions transiting the United States) that involve any property or interests in property of designated or blocked persons. U.S. persons must comply with OFAC regulations, including all U.S. citizens and permanent resident aliens regardless of where they are located, all persons within the United States, and all U.S.- incorporated entities and their foreign branches. Non-U.S. persons are also subject to certain OFAC prohibitions. For example, non-U.S. persons are prohibited from causing or conspiring to cause U.S. persons to wittingly or unwittingly violate U.S. sanctions, as well as engaging in conduct that evades U.S. sanctions. Violations of OFAC regulations may result in civil or criminal penalties. OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if such person did not know or have reason to know that it was engaging in a transaction that was prohibited under sanctions laws and regulations administered by OFAC. OFAC's Economic Sanctions Enforcement Guidelines provide more information regarding OFAC's enforcement of U.S. economic sanctions, including the factors that OFAC generally considers when determining an appropriate response to an apparent violation. For additional information on complying with U.S. sanctions and export control laws, please see Department of Commerce, Department of the Treasury, and Department of Justice Tri-Seal Compliance Note.

(*Continued On The Following Page)

Furthermore, engaging in certain transactions with the individuals designated today entails risk of secondary sanctions pursuant to E.O. 13224, as amended. Pursuant to this authority, OFAC can prohibit or impose strict conditions on the opening or maintaining in the United States of a correspondent account or a payable-through account of a foreign financial institution that knowingly conducted or facilitated any significant transaction on behalf of a Specially Designated Global Terrorist.

The power and integrity of OFAC sanctions derive not only from OFAC's ability to designate and add persons to the SDN List, but also from its willingness to remove persons from the SDN List consistent with the law. The ultimate goal of sanctions is not to punish, but to bring about a positive change in behavior.

****

TRAVEL ADVISORY US STATE DEPT

Lebanon: Travel Advisory Raised to Level 4 — Do Not Travel
07/31/2024 02:33 PM EDT

Office of the Spokesperson
HomeOffice of the SpokespersonPress Releases…Lebanon: Travel Advisory Raised to Level 4 — Do Not Travel hide
Lebanon: Travel Advisory Raised to Level 4 — Do Not Travel
Media Note

July 31, 2024

The Department of State raised the Travel Advisory for Lebanon to Level 4 — Do Not Travel on July 31, 2024. The Department continues to advise travelers not to travel to Lebanon. This replaces the previous Travel Advisory issued on January 29, 2024.

The full text of the updated Travel Advisory is as follows:
July 31, 2024

Updated to raise the Travel Advisory to Level 4: Do Not Travel, due to rising tensions between Hizballah and Israel.

Do Not Travel to Lebanon due to rising tensions between Hizballah and Israel. If you are in Lebanon, be prepared to shelter in place should the situation deteriorate. The U.S. Embassy strongly encourages U.S. citizens who are already in Southern Lebanon, near the borders with Syria, and/or in refugee settlements to depart.
Do Not Travel to Lebanon due to crime, terrorism, civil unrest, kidnapping, unexploded landmines, and the risk of armed conflict. Some areas, especially near the borders, have increased risk. Read the entire Travel Advisory.

Country Summary: Country Summary: U.S. citizens already in Lebanon should be aware of the risks of remaining in the country and review their personal security plans.

U.S. citizens in Lebanon should be aware that consular officers from the U.S. Embassy are not always able to travel to assist them. The Department of State considers the threat to U.S. government personnel in Beirut serious enough to require them to live and work under strict security. The internal security policies of the U.S. Embassy may be adjusted at any time and without advance notice.

(*Continued On The Following Column)

Since October 8, Hizballah has conducted attacks against Israel that have escalated in recent weeks, culminating in a July 27 rocket attack on Majdal Shams, a town in the Golan Heights, which killed 12 children. This strike has increased the risk of further escalation between Hizballah and Israel.

The Lebanese government cannot guarantee the safety of U.S. citizens against sudden outbreaks of violence and armed conflict. Family, neighborhood, or sectarian disputes can escalate quickly and can lead to gunfire or other violence with no warning.

Terrorist groups continue plotting possible attacks in Lebanon. Terrorists may conduct attacks with little or no warning targeting tourist locations, transportation hubs, markets/shopping malls, and local government facilities.

Local security authorities have noted a rise in violent crimes, including political violence. Multiple unsolved killings in Lebanon may have been politically motivated.

Kidnapping, whether for ransom, political motives, or family disputes, has occurred in Lebanon. Suspects in kidnappings may have ties to terrorist or criminal organizations.

Unexploded landmines and explosive remnants of war are a hazard along the border with Syria. Heed land mine warning signs. Do not venture off the road into areas marked off with red and white plastic tape. Avoid roadside ditches, shoulders, and unmarked trails. Never touch anything resembling unexploded munitions.

U.S. citizens should avoid demonstrations and exercise caution if in the vicinity of any large gatherings or protests as these have the potential to turn violent quickly and with little notice. Protesters have blocked major roads, including thoroughfares between downtown Beirut and the area where the U.S. Embassy is located, and between Beirut and Beirut Rafic Hariri International Airport.

Read the country information page for additional information on travel to Lebanon.

If you decide to travel to Lebanon:

- Visit our website for information on Travel to High-Risk Areas.
- Appoint one family member to serve as the point of contact with kidnappers/hostage-takers, media, U.S. and host country government agencies, and members of Congress if you are kidnapped, or taken hostage.
- Keep travel documents up to date and easily accessible.
- Do not touch unknown metal objects and avoid traveling off well-used roads, tracks, and paths due to risk of unexploded ordnance.
- Avoid demonstrations and crowds.
- Stay alert in locations frequented by Westerners.
- Monitor local media for breaking events and adjust your plans based on new information.
- Enroll in the Smart Traveler Enrollment Program (STEP) to receive Alerts and make it easier to locate you in an emergency.
- Follow the Department of State on Facebook and Twitter *(X)*.
- Review the Country Security Report for Lebanon.
- Visit the CDC page for the latest Travel Health Information related to your travel.

(*Continued On The Following Page)

- U.S. citizens who travel abroad should always have a contingency plan for emergency situations. Review the Traveler's Checklist.

Southern Lebanon – Level 4: Do Not Travel, Depart If You Are There
The U.S. Embassy strongly urges U.S. citizens to avoid southern Lebanon and to depart if you are there; that is, all parts south of the city of Saida, to include inland areas, as illustrated in this map. Cross-border rocket, missile, and artillery fire continues to impact southern Lebanon on a daily basis and has caused a significant number of fatalities and injuries.

Border with Syria – Level 4: Do Not Travel, Depart If You Are There
The U.S. Embassy strongly urges U.S. citizens to avoid the Lebanon-Syria border and to depart if you are there. This area has seen clashes between Lebanese security forces and Syrian-based violent extremist groups. The U.S. Department of State also warns U.S. citizens of the risk of traveling on flights that fly over Syria, which include some flights to and from Beirut.

Refugee Settlements – Level 4: Do Not Travel, Depart If You Are There
The U.S. Embassy urges U.S. citizens to avoid travel to refugee settlements in Lebanon and depart if you are there. These settlements are prone to outbreaks of violence including shootings and explosions.

Visit our website for Travel to High-Risk Areas.
****

VIEWS ON POTENTIAL FOR Middle East WAR ESCALATION

July 31, 2024
Ever Closer to War
The Middle East has moved significantly closer to a larger, potentially region-engulfing war.

The sequence in recent days has been dizzying. A quick recap: Since Oct. 8, Israel has engaged in relatively low-grade tit-for-tat strikes with the Lebanese militia Hezbollah, which began firing rockets at Israel in solidarity with Hamas at the Gaza war's outset. (Both Hezbollah and Hamas are Islamist groups backed by Iran as components of its so-called "axis of resistance.") Israel responded by striking Hezbollah commanders in Lebanon. On Saturday, the conflict between the two parties escalated sharply when a rocket killed children on a soccer field in the Golan Heights—an Israeli-controlled area between Israel, Lebanon and Syria. Israel responded by killing a Hezbollah commander deep inside Lebanon, in the southern part of its capital Beirut.

Yesterday brought another turn. Hamas political leader Ismail Haniyeh was killed in Tehran where he had attended the inauguration of Iran's new reformist president this week. "We are on the verge of a large, large-scale escalation," Danni Citrinowicz of the Tel Aviv-based Institute for National Security Studies tells The Wall Street Journal's Summer Said and Rory Jones. "Iran is leading the axis, and they cannot protect one of the leaders of the axis coming for [incoming President Masoud] Pezeshkian's inauguration."

At the Financial Times, Andrew England reminds readers that a war between Israel and Hezbollah could draw in Iran and its other proxies in Gaza and Yemen—and the US, as Israel's strongest defender. "It is the nightmare scenario the regional powers have been warning of for the duration of Israel's war in Gaza," England writes. Cautioning that the "Middle East must step back from the brink," The Economist urges Israel to reach a ceasefire with Hamas in Gaza and lower the regional temperature.

(*Continued On The Following Column)

Analysts have noted thoroughly the destruction a larger war could cause and the strong incentives for all parties to avoid one. "Iran will find it hard not to retaliate for an assassination on its soil," writes Haaretz columnist Amos Harel. "Until now, however, it seemed both Iran and Hezbollah sought to contain the conflict with Israel and prevent it from turning into an all-out war."

At The Atlantic, Graeme Wood argues counterintuitively that these assassinations will help avoid disaster by raising the stakes and communicating with Tehran and its proxies differently. "Sometimes the one who is willing to bargain with you is not the one who has the authority to make a deal," Wood writes. "Israel can attack the Houthis [in Yemen] and Hezbollah. But Iran is their backer … It seems in this case that Israel found a middle way, by attacking an Iranian ally, on Iranian soil, in such a way as to prove to the other allies that Iran cannot protect them. It implies that the link between the backer and the backed might not be as reliable as either assumed. If that message is received as intended, Haniyeh's assassination will have de-escalated regional tensions rather than ratcheted them up."

Keep up to date with latest trade news at:
www.eib.com

PODCAST LINK:

EIB Export News Episode 22 – NATO 75th Anniversary Summit

https://www.buzzsprout.com/1592353/15500353

MISSION STATEMENT:

Given the geopolitical state of affairs with China, Russia, and Crimea, the Occupied territories of UKRAINE, Donetsk and Luhansk Oblast, embargoed countries and other specific threatening end users and entities, located in the United States and around the globe;

Evolutions in Business and the companies we serve, armed with robust compliance to the Export Administration Regulations, will adhere to best practices to protect our revenue and yours, and ensure the national security interests of the United States.

NOTE: In accordance with Title 17 U.S.C. Section 107, this material is distributed without profit or payment for non-profit news reporting and educational purposes only.

Evolutions in Business

Celebrating more than 30 Years