



ΚΥΠΡΙΑΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΕΞΩΤΕΡΙΚΩΝ

ΠΟΛΙΤΙΚΗ ΔΙΕΥΘΥΝΣΗ

ΤΜΗΜΑ ΠΟΛΥΜΕΡΩΝ ΣΧΕΣΕΩΝ ΚΑΙ ΔΙΕΘΝΩΝ ΟΡΓΑΝΙΣΜΩΝ

Αρ. Φακ: 24.11.002.003, 04.02.004.001.003.001, 04.02.004.001.003.006, 04.01.006

Τηλεμοιότυπο: 22 661881

Ηλεκτρ. Διεύθυνση: amattheou@mfa.gov.cy

Συνημμένα έγγραφα: 5 Παραρτήματα

08 Νοεμβρίου 2018

MA II → Πίνακας Αποδεκτών (ως συνημμένο Παράρτημα Ι)

ΘΕΜΑ: Επιαναφορά αμερικανικών κυρώσεων κατά του Ιράν

1. Επί ανωτέρω θέματος, πληροφορείσθε, ότι στις 05/11/2018 η αμερικανική κυβέρνηση επανέφερε τη δεύτερη δέσμη κυρώσεων έναντι του Ιράν, σε συνέχεια απόφασης Προέδρου Trump στις 08/05/18 για αποχώρηση των Ηνωμένων Πολιτειών από την Συμφωνία για το πυρηνικό πρόγραμμα του Ιράν, γνωστή ως Κοινό Ολοκληρωμένο Σχέδιο Δράσης (JCPOA), η οποία μάλιστα κατοχυρώθηκε ομόφωνα με Ψήφισμα του ΣΑ/ΟΗΕ 2231 (2015).
2. Υπενθυμίζεται, ότι το JCPOA προβλέπει, υπό συγκεκριμένες προϋποθέσεις, τη σταδιακή άρση των διεθνών (και ευρωπαϊκών) κυρώσεων που επιβλήθηκαν από το 2006 και εντεύθεν έναντι του Ιράν λόγω της ανάπτυξης του πυρηνικού του προγράμματος. Περισσότερες πληροφορίες σε σχέση με το ισχύον καθεστώς συνέπεια του Ψηφίσματος 2231 (2018) δύνανται να αντληθούν από τις ιστοσελίδες των Ηνωμένων Εθνών και της Ε.Ε.:
<http://www.un.org/en/sc/2231/>
<https://www.sanctionsmap.eu/#/main/details/18/?search=%7B%22value%22:%22%22.%22searchType%22:%22%7B%7D%7D>
3. Όσον δε αφορά τις αμερικανικές κυρώσεις, υπενθυμίζεται, ότι στις 07/08/2018, οι ΗΠΑ επανέφεραν σε ισχύ την πρώτη δέσμη κυρώσεων κατά του Ιράν με την οποία απαγορεύουν στο Ιράν να εξάγει βιομηχανικά και αγροτικά προϊόντα, να συναλλάσσεται στις διεθνείς αγορές και να εισάγει αυτοκίνητα, αεροπλάνα και τα ανταλλακτικά τους.
4. Η επαναφορά της δεύτερης δέσμης κυρώσεων στις 05/11/18 που σχετίζονται με το JCPOA και η παράλληλη ενίσχυσή τους, αποτελούν, σύμφωνα με τις διακηρύξεις της αμερικανικής κυβέρνησης, τις σκληρότερες και αυστηρότερες κυρώσεις που επιβλήθηκαν ποτέ στο Ιράν και στοχεύουν τον πετρελαϊκό τομέα (απαγόρευση εξαγωγών πετρελαίου και φυσικού αερίου), τον χρηματοπιστωτικό (απαγόρευση χρηματοπιστωτικών οργανισμών να συναλλάσσονται με ιρανικά Τραπεζικά ιδρύματα συμπεριλαμβανομένης της Κεντρικής Τράπεζας του Ιράν) και τον ναυτιλιακό. Απαγορεύεται

επίσης η παροχή μηνυμάτων χρηματοοικονομικού περιεχομένου μέσω SWIFT στην Κεντρική Τράπεζα του Ιράν και σε συγκεκριμένα ιρανικά χρηματοπιστωτικά ιδρύματα, καθώς και η παροχή υπηρεσιών ασφάλισης, αντασφάλισης και αναδοχής (*underwriting services*).

5. Στο πλαίσιο αυτό, το αμερικανικό Υπουργείο Οικονομικών (OFAC) καταχώρησε στον κατάλογο των *Specially Designated Nationals and Blocked Persons (SDN List)* περισσότερα από 700 πρόσωπα, οντότητες, πλοία και αεροπορικές εταιρείες, συμπεριλαμβανομένων μεγάλων ιρανικών τραπεζών, εξαγωγέων πετρελαίου και ναυτιλιακών εταιρειών που συνδέονται καθ' οιονδήποτε τρόπο με την κυβέρνηση του Ιράν. Πρόκειται τόσο για επαναφορά των κυρώσεων σε όλους όσοι αφαιρέθηκαν από τους καταλόγους το 2016 συνεπεία του JPCOA αλλά και για περίπου 300 νέες καταχωρήσεις. Για περισσότερες πληροφορίες σε σχέση με τα στοχευμένα πρόσωπα μπορείτε να ανατρέξετε στην ιστοσελίδα της OFAC: https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20181105_names.aspx
6. Στόχος της χρήσης των ως άνω δευτερογενών κυρώσεων ΗΠΑ είναι η άσκηση μέγιστης πίεσης στο Ιράν για αλλαγή πολιτικής μέσω της οικονομικής απομόνωσής του. Ως εκ τούτου, ο σχεδιασμός των επιβλητέων κυρώσεων αποσκοπεί στον αποκλεισμό των στοχευμένων προσώπων και οντοτήτων και όσων προσπαθούν να παρακάμψουν τις κυρώσεις με το να συνεργάζονται / δραστηριοποιούνται μαζί τους, από κάθε οικονομική δοσοληψία με οικονομικούς φορείς στις ΗΠΑ, καθώς και τον αποκλεισμό τους από το αμερικανικό χρηματοπιστωτικό σύστημα, συμπεριλαμβανομένης της χρήσης του αμερικανικού δολαρίου ως συναλλαγματικής μονάδας (η γνωστή εξωεδαφική ισχύ των αμερικανικών κυρώσεων).
7. Ωστόσο η α/κυβέρνηση διαβεβαίωσε, ότι θα διατηρήσει περιορισμένες εξαιρέσεις για ανθρωπιστικούς λόγους (*humanitarian exemptions*), που αφορούν στην προμήθεια τροφίμων, αγροτικών προϊόντων (*agriculture commodities*), φαρμάκων και ιατρικού εξοπλισμού (βλ. στις *Frequently Asked Questions (FAQs)* της OFAC την απάντηση υπ' αριθμ. 637 - σχετικός σύνδεσμος παρατίθεται κάτωθι).
8. Λόγω ειδικών περιστάσεων και για να διασφαλισθεί ο ενεργειακός εφοδιασμός, οι ΗΠΑ συμφώνησαν να παράσχουν προσωρινή εξαίρεση από την απαγόρευση προμήθειας ιρανικού αργού πετρελαίου σε επτά χώρες, ήτοι Ιαπωνία, Κίνα συμπεριλαμβανομένης της Ταϊβάν, Δημοκρατία Κορέας (Νότιος Κορέα), Ινδία, Ελλάδα, Ιταλία και Τουρκία, οι οποίες έχουν ήδη μειώσει σημαντικά τις εισαγωγές ιρανικού πετρελαίου. Στόχος ΗΠΑ όπως οι εν λόγω εισαγωγές μηδενιστούν.
9. Για πιο ολοκληρωμένη εικόνα, περισσότερες πληροφορίες σε σχέση με την επαναφορά και ενίσχυση των αμερικανικών κυρώσεων έναντι του Ιράν μπορείτε να αντλήσετε από τους κάτωθι συνδέσμους:

<https://www.treasury.gov/resource-center/sanctions/Programs/pages/iran.aspx>

https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_iran.aspx#630 (*Frequently Asked Questions Related to the "Snap-back" of Iranian sanctions in November, 2018*, βλ. Ερωτήσεις 256, 417, 630 -- 645)

<https://www.state.gov/secretary/remarks/2018/11/287132.htm>

<https://www.state.gov/secretary/remarks/2018/11/287090.htm>

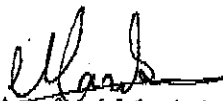
<https://www.state.gov/r/pa/prs/ps/2018/11/287095.htm>

- 10. Επισυνάπτονται δε, δυο ενημερωτικά έγγραφα (ΠΑΡ. II και III) που μας ενεχείρισε η εδώ Αμερικανική Πρεσβεία.

Αντίδραση Ε.Ε.:

11. Επισημαίνεται κατ' αρχάς ο μη δεσμευτικός χαρακτήρας των κυρώσεων ΗΠΑ, παρά την εξωεδαφική ισχύ τους. Ωστόσο, εντός της Ε.Ε., επικρατεί ιδιαίτερη ανησυχία σε σχέση με τις δευτερογενείς κυρώσεις ΗΠΑ που σχετίζονταν με το πυρηνικό πρόγραμμα του Ιράν και που δύναται να εφαρμοστούν σε μη-Αμερικανούς, που λειτουργούν εκτός δικαιοδοσίας ΗΠΑ (εξωεδαφική ισχύ).
12. Στο πλαίσιο αυτό, με την επαναφορά της πρώτης δέσμης αμερικανικών κυρώσεων, η Ε.Ε. έλαβε μέτρα προστασίας των ευρωπαϊκών οικονομικών παραγόντων που εμπλέκονται σε νόμιμες επιχειρηματικές δραστηριότητες με το Ιράν σύμφωνα με το Δίκαιο της Ε.Ε. και το Ψήφισμα ΣΑ/ΟΗΕ 2231(2015), όπως για παράδειγμα την επικαιροποίηση της νομοθεσίας θωράκισης (*EU blocking statute*)¹, με στόχο την προστασία των ευρωπαϊκών εταιρειών από τις αρνητικές συνέπειες απόφασης ΗΠΑ.
- 13. Για διευκόλυνση επισυνάπτεται ενημερωτικό έγγραφο (ΠΑΡ. VI) με όλες τις σχετικές πληροφορίες για τη νομοθεσία θωράκισης, οι οποίες αντλήθηκαν από την ιστοσελίδα της Ε.Ε. Σημειώνεται δε, ότι λόγω του ότι η νομοθεσία θωράκισης εμπίπτει στο πεδίο εφαρμογής της κοινής εμπορικής πολιτικής (νομικές βάσεις άρθρα 64, 207 και 352 της Συνθήκης για τη Λειτουργία της Ε.Ε.), η εφαρμοστέα αρχή θεωρείται το Υπουργείο Εμπορίου.
14. Αναφέρεται, τέλος, ότι λίγο πριν την επίσημη επιβολή της δεύτερης δέσμης κυρώσεων στις 05/11/18, προηγήθηκε Κοινή Ανακοίνωση (επισυνάπτεται ως ΠΑΡ. V) της Υπατης Εκπροσώπου και Αντιπροέδρου Ευρ. Επιτροπής (ΥΑ/ΑΕ) κας Mogherini και των Υπουργών Εξωτερικών της Γαλλίας, Γερμανίας και Ηνωμένου Βασιλείου (Ε3), η οποία, μεταξύ άλλων, κάνει λόγο για έναρξη συζητήσεων για τη δημιουργία ενός Ειδικού Μηχανισμού (*Special Purpose Vehicle*), με σκοπό την διαφύλαξη και διατήρηση αποτελεσματικών χρηματοοικονομικών καναλιών με το Ιράν, και τη συνέχιση των εξαγωγών ιρανικού πετρελαίου και φυσικού αερίου.

Τα ανωτέρω για την ενημέρωσή σας.


Αγγελική Ματθαίου
Για Γενικό Διευθυντή

¹ Κανονισμός (ΕΚ) αριθ. 2271/96 του Συμβουλίου, της 22^{ης} Νοεμβρίου 1996, για την προστασία από τις συνέπειες της εξωεδαφικής εφαρμογής ορισμένων νόμων.

ΠΑΡΑΡΤΗΜΑ Ι - ΠΙΝΑΚΑΣ Αποδεκτών

- Γενικό Εισαγγελέα της Δημοκρατίας
(Προϊστάμενη ΜΟΚΑΣ, Προϊστάμενη Τομέα Δικαίου ΕΕ)
- Διοικητή Κεντρικής Τράπεζας της Κύπρου
- ΓΔ Υπουργείου Οικονομικών
(Δ/ντή Τμήματος Τελωνείων, Διευθύντρια Υπηρεσίας Ελέγχου Ασφαλιστικών Εταιρειών, Δ/ντή Τμήματος Χρηματοδότησης και Επενδύσεων, Δ/ντή Τμήματος Φορολογίας)
- ΓΔ Υπουργείου Εσωτερικών
(Δ/ντή Τμήματος Κτηματολογίου και Χωρομετρίας, Δ/ντή Τμήματος Αρχείου Πληθυσμού και Μετανάστευσης)
- ΓΔ Υπουργείου Άμυνας
- ΓΔ Υπουργείου Δικαιοσύνης και Δημόσιας Τάξης
- ΓΔ Υπουργείου Μεταφορών, Επικοινωνιών και Έργων
(Δ/ντή Πολιτικής Αεροπορίας)
- ΓΔ Υπουργείου Ενέργειας, Εμπορίου, Βιομηχανίας και Τουρισμού
(Εφορο Εταιρειών και Επίσημο Παραλήπτη, Διευθύντρια Υπηρεσίας Εμπορίου, Δ/ντή Υπηρεσίας Ενέργειας, Προϊστάμενο Κλάδου Αδειών Εισαγωγών / Εξαγωγών)
- Αν. Γενικό Διευθυντή Υφυπουργείου Ναυτιλίας
- Αρχηγό Αστυνομίας (ΔΕΕ & ΔΑΣ)
- Διοικητή ΚΥΠ
- ΓΔ Αρχής Λιμένων Κύπρου
- Πρόεδρο Επιτροπής Κεφαλαιαγοράς Κύπρου
- EUROGATE CONTAINER TERMINAL LIMASSOL LTD (Αρ. Φαξ: 25 577434)
- DP WORLD LIMASSOL LTD (Αρ. Φαξ: 25 661314)
- P & O MARITIME CYPRUS LTD (Email: jim.maitland@pomaritime.com)

Κοινοποίηση (για ενημέρωση):

- Πρόεδρο Παγκύπριου Δικηγορικού Συλλόγου
- Πρόεδρο Συνδέσμου Εγκριμένων Λογιστών
- Πρόεδρο Κυπριακού Οργανισμού Προσέλκυσης Επενδύσεων (CIPA)
- Πρόεδρο Εμπορικού και Βιομηχανικού Επιμελητηρίου
- Πρόεδρο Συνδέσμου Ασφαλιστικών Εταιρειών Κύπρου
- Γενικό Διευθυντή Ομοσπονδίας Εργοδοτών και Βιομηχάνων
- ΑΔΑ - ΓΕΝ 544/18
- ΓΥ, ΓΓΔ, Πολιτικό Διευθυντή, Δ/ντή Δ, ΕΑ
- ΔΔΓΠΤΔ Α/Α 2203/18

ΠΑΡΑΡΤΗΜΑ II

CBI Officials

- (U) Senior officials of the Central Bank of Iran (CBI) conduct transactions for the benefit of the Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF), Lebanese Hizballah, and other terrorist groups by using regional financial institutions to conceal the illicit nature of these transactions. Financial institutions should be aware that some counterparty financial institutions may not be equipped to identify CBI officials' deceptive transactions, which include the use of personal bank accounts.
 - (U) For example, on May 15, 2018, the Office of Foreign Assets Control (OFAC) designated then-CBI Governor Valiollah Seif and the assistant director of the CBI's International Department Ali Tarzali for conducting transactions through Iraq's banking sector for the IRGC-QF and Lebanese Hizballah.

Exchange Houses

- (U) Financial institutions are advised to exercise appropriate due diligence when dealing with transactions involving exchange houses that may have exposure to Iran or Iranian persons. The Iranian regime uses exchange houses to facilitate malign activity—including by couriering cash to third-country exchange houses, using the exchange houses to convert it to various currencies, and delivering these currencies to the IRGC-QF and its proxies to fund their operations worldwide. These practices also include third-country exchange houses or trading companies acting as money transmitters in processing funds transfers through the U.S. to third-country beneficiaries, in support of unauthorized Iranian business. Given Iran's heavy reliance on exchange houses to evade sanctions during previous periods of heightened sanctions pressure, Iran will likely increase the use of this evasive practice as sanctions previously lifted under the JCPOA are re-imposed.
 - (U) For example, on May 10, 2018, the United States and the United Arab Emirates jointly disrupted an extensive network of currency exchange houses in Iran and the UAE, with OFAC designating individuals and entities that converted other currency to U.S. dollar-denominated bulk cash for the benefit of the IRGC-QF by using front companies and other deceptive practices to hide the illicit nature of the scheme.

Procurement

- (U) Iran's procurement networks use front and shell companies around the world to obtain goods and services in evasion of sanctions and in furtherance of ballistic missile proliferation, currency counterfeiting, and other destabilizing activities.
 - (U) For example, in February 2017, OFAC designated individuals and entities in the Abdollah Asgharzadeh network for using China-based brokers to obfuscate

the nature of transactions to make dual-use and other goods available for Iran's ballistic missile programs.

- (U) For example, in November 2017, OFAC designated certain individuals and entities for using Germany-based front companies to deceive European suppliers, circumvent European export restrictions, and procure advanced machinery and necessary raw materials, which enabled the network to print counterfeit Yemeni bank notes for the IRGC-QF.

Commercial Aviation Industry & Mahan Air

- (U) Designated Iranian airlines and their agents and affiliates use front companies in deceptive schemes to procure aviation-related materials in violation of sanctions. Financial institutions are advised to exercise appropriate due diligence given that they may be subject to sanctions for knowingly conducting transactions for or with certain Iran-related persons or entities (such as Mahan Air).
- (U) Specifically, Mahan Air has for many years transferred weapons, funds, and people for the IRGC-QF and provided support to the Syrian Assad regime and Lebanese Hizballah. To do so, its agents and affiliates have moved payments through front companies and financial institutions throughout the U.S., Europe, and Asia, and other countries in evasion of sanctions. On May 24, 2018, for example, OFAC designated a network of Turkish front companies that procured U.S.-origin, export-controlled parts for Mahan Air via Istanbul. Further, on July 9, 2018, OFAC designated a Malaysia-based general sales agent that provided Mahan with reservation and ticketing services. This action underscored for the aviation community the sanctions risk of maintaining commercial relationships with Mahan Air and other designated Iranian airlines.

Shipping Companies

- (U) Iran has also used deceptive shipping practices to access the financial system for illicit purposes and will likely increase its reliance on methods of sanctions evasion involving shipping companies as sanctions lifted under the JCPOA are re-imposed. Specifically, these methods to obfuscate illicit transactions include use of falsified documents, such as bills of lading, shipping invoices, and vessel registration; reflagging of vessels to hide origin and purpose; third parties, such as brokers and trading companies, as well as front companies or individuals acting on behalf of newly-designated persons. Financial institutions may find maritime databases and reports helpful when verifying trade-related documents.

Precious Metals

- (U) Iran has previously used trade in precious metals such as gold to facilitate the sale of Iranian oil and other goods abroad, obfuscate the real beneficiaries of these proceeds, and fund the regime's malign activities via financial systems worldwide. Financial institutions should be aware of these sanctions evasion schemes.

Virtual Currency

- (U) In light of the fact that Iran has already transacted at least \$3.8 million-worth of bitcoin yearly since 2013, institutions should conduct due diligence with the recognition that virtual currency is an emerging payments system with potential avenues for sanctions evasion. Activity of virtual currency exchanges may involve wire transactions from several disparate accounts or locations combined with transfer to or from virtual currency exchanges. As relevant to foreign financial institutions' understanding of their U.S. correspondents' obligations, U.S. persons are subject to compliance obligations regardless of whether a transaction is denominated in virtual currency.

Findings of the Financial Action Task Force (FATF)

- (U) In June 2018, the FATF publicly noted Iran's failure to implement a previously agreed-upon action plan to address its AML/CFT deficiencies and reiterated its concern with the terrorist financing risk emanating from Iran to the international financial system. Specifically, as the FATF has stated publicly, Iran still lacks an adequate and enforceable customer due diligence regime. Given the ongoing deficiencies in their AML/CFT regime that even recent legislation has failed to address, the FATF urges all jurisdictions to continue to advise their financial institutions to apply enhanced due diligence to business relationships and transactions with natural and legal persons from Iran.

Red Flags

- (U) The advisory describes 21 red flags that may assist financial institutions in identifying the methods by which the Iranian regime tries to exploit the international financial system. These include:
 - Unusual wire transfers, such as those involving the CBI unrelated to traditional central bank activity;
 - Use of multiple exchange houses, incurring atypical and unnecessary costs;
 - Multiple depositors that do not appear to match an account holder's profile, particularly involving exchange houses;
 - Shell or front companies—which may originate with or be directed to shell corporations, general “trading companies,” or companies with a nexus to Iran—for use in procurement networks;
 - Unrelated business, including transactions that do not comport with CDD, used in connection with procurement networks;
 - Misrepresentation of sanctions to suppliers, dealers, brokers, re-insurers, and other intermediaries, as well as false claims without supporting documentation that OFAC licenses have been obtained, in particular illicitly to procure aircraft parts;
 - Inconsistent documentation for vessels using key ports, including omissions in shipping documents of docking in Iranian ports, as potentially indicated otherwise by maritime database entries;

- Lack of information regarding origin of funds, including wire transfers or deposits involving China, Hong Kong, Iraq, Russia, Turkey, the UAE, and other jurisdictions with higher risk of dealing with entities linked to Iran;
- Logins from Iranian internet protocol addresses or with Iranian email to transact virtual currencies, as well as other technical details indicating a nexus to Iran.

Snap-Back of U.S. Sanctions

- (U) The advisory also reminds financial institutions of the snap-back of U.S. sanctions on Iran as a result of the United States' departure from the JCPOA. These measures consist of:
 - (U) Sanctions that were re-imposed after the 90-day wind-down period, which ended on August 6, 2018:
 - i. Sanctions on the purchase or acquisition of U.S. dollar banknotes by the Government of Iran;
 - ii. Sanctions on Iran's trade in gold or precious metals;
 - iii. Sanctions on the direct or indirect sale, supply, or transfer to or from Iran of graphite, raw, or semi-finished metals such as aluminum and steel, coal, and software for integrating industrial processes;
 - iv. Sanctions on significant transactions related to the purchase or sale of Iranian rials, or the maintenance of significant funds or accounts outside the territory of Iran denominated in the Iranian rial;
 - v. Sanctions on the purchase, subscription to, or facilitation of the issuance of Iranian sovereign debt; and
 - vi. Sanctions on Iran's automotive sector.
 - (U) The revocation of specific licenses issued under the *Statement of Licensing Policy for Activities Related to the Export or Re-export to Iran of Commercial Passenger Aircraft and Related Parts and Services* (JCPOA SLP).
 - (U) The U.S. government has amended and/or revoked the following JCPOA-related authorizations under U.S. primary sanctions regarding Iran:
 - i. OFAC amended the Iranian Transactions and Sanctions Regulations (ITSR) to narrow the scope of the general licenses at 31 C.F.R. part 560.534 and 560.535 to authorize the wind down, through August 6, 2018, of the importation into the United States of Iranian-origin carpets and foodstuffs and certain related financial transactions.
 - ii. OFAC revoked General License I and issued a wind-down general license that authorized, through August 6, 2018, the wind down of activities relating to contingent contracts for activities eligible for authorization under the JCPOA SLP that were previously authorized pursuant to General License I.

iii. OFAC has revoked General License H and issued a wind-down general license that authorizes, through November 4, 2018, the wind down of activities involving U.S.-owned or -controlled foreign entities and the Government of Iran or persons subject to the jurisdiction of the Government of Iran that were previously authorized pursuant to General License H.

- (U) Sanctions to be re-imposed after the 180-day wind-down period ending on November 4, 2018:

i. Sanctions on Iran's port operators, and shipping and shipbuilding sectors, including on the Islamic Republic of Iran Shipping Lines (IRISL), South Shipping Line Iran, or their affiliates;

ii. Sanctions on petroleum-related transactions with, among others, the National Iranian Oil Company (NIOC), Naftiran Intertrade Company (NICO), and National Iranian Tanker Company (NITC), including the purchase of petroleum, petroleum products, or petrochemical products from Iran;

iii. Sanctions on transactions by foreign financial institutions with the Central Bank of Iran and designated Iranian financial institutions under Section 1245 of the National Defense Authorization Act for Fiscal Year 2012 (NDAA);

iv. Sanctions on the provision of specialized financial messaging services to the Central Bank of Iran and Iranian financial institutions described in Section 104(c)(2)(E)(ii) of the Comprehensive Iran Sanctions and Divestment Act of 2010 (CISADA);

v. Sanctions on the provision of underwriting services, insurance, or reinsurance; and

vi. Sanctions on Iran's energy sector.

- (U) Furthermore, no later than November 5, 2018, the U.S. government will re-impose, as appropriate, the sanctions that applied to persons removed from the List of Specially Designated Nationals and Blocked Persons (SDN List) and/or other lists maintained by the U.S. government on January 16, 2016.



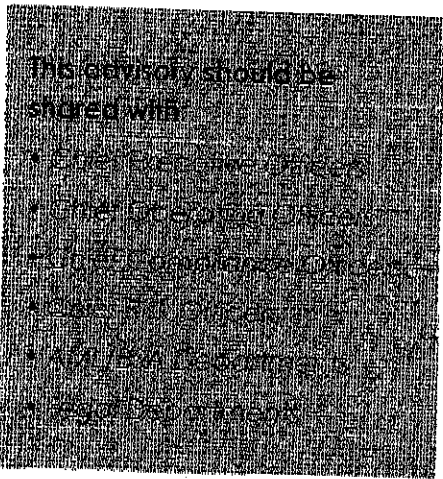
FinCEN ADVISORY

FIN-2018-A006

October 11, 2018

Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to help U.S. financial institutions (particularly banks; money services businesses (MSBs), such as virtual currency administrators and exchangers; and dealers in precious metals, stones, and jewels) better detect potentially illicit transactions related to the Islamic Republic of Iran (Iran). This advisory will also help foreign financial institutions better understand the obligations of their U.S. correspondents, avoid exposure to U.S. sanctions, and address the Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) risks that Iranian activity poses to the international financial system.¹



The Iranian regime has long used front and shell companies to exploit financial systems around the world to generate revenues and transfer funds in support of malign conduct, which includes support to terrorist groups, ballistic missile development, human rights abuses, support to the Syrian regime, and other destabilizing actions targeted by U.S. sanctions.

This advisory highlights the Iranian regime's exploitation of financial institutions worldwide, and describes a number of typologies used by the regime to illicitly access the international financial system and obscure and further its malign activity. It also provides red flags that may assist financial institutions in identifying these methods.² Additionally, this advisory is intended to assist financial institutions in light of the United States' withdrawal from the Joint Comprehensive Plan of Action (JCPOA) and the re-imposition of U.S. sanctions previously lifted under the JCPOA following the 90- and 180-day wind-down periods for certain activities, while also reminding financial institutions of regulatory obligations under the Bank Secrecy Act (BSA) and the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (CISADA).³

1. For general information on U.S. sanctions on Iran, see the "U.S. Sanctions" section on p.15 of this advisory.
2. While this advisory addresses U.S. sanctions that prohibit U.S. persons and U.S.-owned or -controlled foreign entities from engaging in transactions involving Iran, including persons "ordinarily resident" in Iran, financial institutions should not take this to mean that all transactions involving Iran, Iranian citizens, or persons with connections to Iran are suspicious or prohibited. Institutions should instead regard an Iranian nexus and the typologies listed in this advisory as factors to consider when assessing whether any specific transaction or activity has an illicit nexus or is otherwise prohibited.
3. For more information about the withdrawal of the United States from the JCPOA, please see <https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20180508.aspx> and <https://www.treasury.gov/resource-center/sanctions/Programs/Pages/iran.aspx>.

Iran's Abuse of the International Financial System

Some of the methods used by the Iranian regime to access the financial system through covert means and to further its malign activities include misusing banks and exchange houses, operating procurement networks that utilize front or shell companies, exploiting commercial shipping, and masking illicit transactions using senior officials, including those at the Central Bank of Iran (CBI). Iran also has a history of using precious metals to evade sanctions and gain access to the financial system and may seek to use virtual currencies in the future. Often, these efforts serve to fund the regime's nefarious activities, including providing funds to the Islamic Revolutionary Guard Corps (IRGC) and its Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF), as well to Lebanese Hizballah, Hamas, and other terrorist groups.

The Iranian Regime's Use of CBI Officials and Exchange Houses to Facilitate Malign Activity

Use of CBI Officials

Senior officials of the CBI have played a critical role in enabling illicit networks, using their official capacity to procure hard currency and conduct transactions for the benefit of the IRGC-QF and its terrorist proxy group, Lebanese Hizballah.⁴ The CBI has also been complicit in these activities.

On May 15, 2018, the Office of Foreign Assets Control (OFAC) designated then-CBI Governor Valiollah Seif and the assistant director of the CBI's International Department, Ali Tarzali, adding them to OFAC's List of Specially Designated Nationals and Blocked Persons (SDN List) for conducting transactions through Iraq's banking sector for the benefit of the IRGC-QF and Lebanese Hizballah, which has acted as a proxy for the IRGC-QF.⁵ Specifically, Valiollah Seif conspired with the IRGC-QF to move millions of dollars, in a variety of currencies, through the international financial system to allow the IRGC-QF to fund its activities abroad. Seif also supported the transfer of IRGC-QF-associated funds to al-Bilad Islamic Bank, an Iraq-based bank that was also designated by OFAC. Ali Tarzali worked with Lebanese Hizballah and proposed that the terrorist group send funds through al-Bilad Islamic Bank. On May 15, 2018, OFAC also designated the Chairman and Chief Executive of al-Bilad Islamic Bank, who acted as an intermediary to enable and conceal these transactions.⁶

Financial institutions should be aware that the U.S. Department of the Treasury has repeatedly observed CBI officials and the IRGC-QF using regional financial institutions as intermediaries to conceal illicit transactions. In exercising appropriate due diligence, financial institutions should be

4. See <https://home.treasury.gov/index.php/news/press-releases/sm0385>. In addition, on May 13, 2018 and May 17, 2018, OFAC issued new designations relating to the Central Bank of Iran and its senior officials.

5. See <https://home.treasury.gov/news/press-releases/sm0385>.

6. See <https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20180515.aspx> and <https://home.treasury.gov/index.php/news/press-releases/sm0385>.

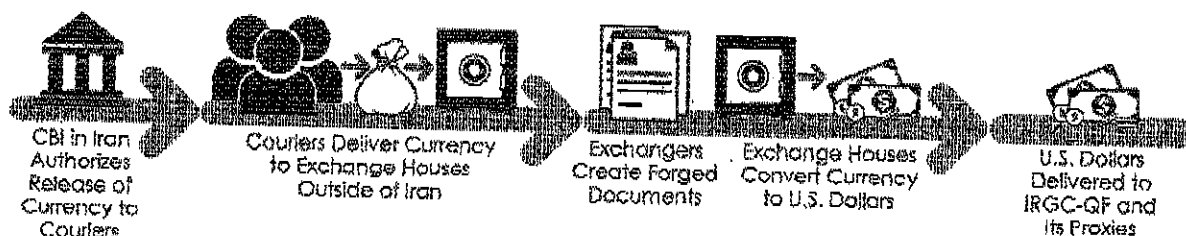
aware that some counterparty financial institutions may not be equipped to identify or address CBI officials' deceptive transactions.⁷ IRGC-QF front companies are known to retrieve funds—some of which are generated by the sale of Iranian oil—in various currencies from foreign bank accounts held by the CBI and then transfer the funds back to Iran.

Use of Exchange Houses

Financial institutions are also advised to exercise appropriate due diligence when dealing with transactions involving exchange houses that may have exposure to Iran or Iranian persons, given that the Iranian regime, senior CBI officials, and the CBI have used such entities to conceal the origin of funds and procure foreign currency for the IRGC-QF.

For example, on May 10, 2018, the United States, in a joint action with the United Arab Emirates (UAE), disrupted an extensive currency exchange network in Iran and the UAE. The network procured and then transferred millions of U.S. dollar-denominated bulk cash through the UAE to the IRGC-QF. As part of this joint action, OFAC designated six individuals and three entities, including Jahan Aras Kish, the Joint Partnership of Mohammadreza Khedmati and Associates, and the Rashed Exchange.⁸ The CBI was complicit in the IRGC-QF's scheme, actively supported this network's currency conversion, and enabled it to access funds that it held in its foreign bank accounts. To mask ties to Iran and particularly to the IRGC-QF, this network of cash couriers and currency exchangers established the three now-designated front companies. At least one of these companies, the Rashed Exchange, advertised its currency exchange and international money transfer business all over the world on its website and through social media in an effort to portray its activities as legitimate, while in reality its management was using the company to facilitate the transfers for the IRGC-QF. Khedmati, the managing director of Rashed Exchange, also worked with the IRGC-QF to forge documents to conceal their illicit financial activities from UAE authorities. Using these front companies, these individuals and entities procured and transferred millions in U.S. dollar-denominated bulk cash to the IRGC-QF to fund its malign activities and regional proxy groups.⁹

The diagram below depicts this type of exchange house-related scheme:



7. See <https://home.treasury.gov/news/press-releases/sm0383>.

8. *Ibid.*

9. See <https://home.treasury.gov/index.php/news/press-releases/sm0385>.

F I N C E N A D V I S O R Y

As financial institutions are aware, during previous periods of heightened sanctions pressure, Iran relied heavily on third-country exchange houses and trading companies to move funds to evade sanctions.¹⁰ As the sanctions on Iran that were lifted under the JCPOA are coming back into effect, Iranian financial institutions can be expected to increase the use of these or other evasive practices. These practices include the use of third-country exchange houses or trading companies to act as money transmitters in processing funds transfers through the United States to third-country beneficiaries, in support of business with Iran that is not exempt or otherwise authorized by OFAC. These third-country exchange houses or trading companies frequently lack their own U.S. dollar accounts and instead rely on the correspondent accounts of their regional banks to access the U.S. financial system. Often these entities are located in jurisdictions considered high risk for transactions implicating OFAC sanctions, and they appear to process primarily commercial transactions rather than personal remittances, which are authorized by OFAC.

OFAC's January 10, 2013 advisory identified the following evasive practices used by such third-country exchange houses or trading companies: omission of references to Iranian addresses, omission of names of Iranian persons or entities in the originator or beneficiary fields, and transmission of funds without referencing the involvement of Iran or the designated persons.¹¹

Financial institutions should be aware when monitoring payments involving third-country exchange houses or trading companies that, as informed by such firms' risk profile, a financial institution may be processing commercial transactions related to Iran or Iranian persons. As appropriate, financial institutions should consider (1) requesting additional information from correspondents on the nature of such transactions and the parties involved; (2) while monitoring these payments, conducting account and transaction reviews for individual exchange houses or trading companies that have repeatedly violated or attempted to violate U.S. sanctions against Iran; and (3) contacting their correspondents that maintain accounts for, or facilitate transactions on behalf of, third-country exchange houses or trading companies that engage in one of the above-referenced examples in order to request additional information and to alert them to the use of these practices.

10. Third-country exchange houses are financial institutions licensed to deal in foreign exchange and transmit funds on behalf of individuals and companies. Trading companies are entities that are not licensed to transmit funds, but in practice operate as exchange houses and rely upon their bank accounts to transmit funds on behalf of third parties. See https://www.treasury.gov/resource-center/sanctions/Programs/Documents/20130110_iran_advisory_exchange_house.pdf.

11. In 2013, OFAC issued an advisory that highlighted some of the practices used at that time to circumvent U.S. and international economic sanctions concerning Iran, including relying heavily on third-country exchange houses and trading companies to move funds. See https://www.treasury.gov/resource-center/sanctions/Programs/Documents/20130110_iran_advisory_exchange_house.pdf. Neither the 2013 OFAC advisory nor this advisory are intended to suggest that U.S. financial institutions close accounts they hold for third-country exchange houses and/or trading companies. Additionally, neither advisory should be interpreted as a signal that third-country exchange houses and/or trading companies are necessarily facilitating illicit finance.

Iran's Use of Procurement Networks

Malign Iran-related actors use front and shell companies¹² around the world to procure technology and services that allow them to evade sanctions and continue their destabilizing behaviors. Through these procurement networks, Iran has gained goods and services related to currency counterfeiting, dual-use equipment, and the commercial aviation industry. As part of a risk-based approach, financial institutions should familiarize themselves with these deceptive practices and take steps to avoid direct or indirect facilitation of them.

Printing Equipment and Materials for Counterfeiting Currency

In November 2017, OFAC designated two individuals, Reza Heidari and Mahmoud Seif, and four entities, Pardazesh Tasvir Rayan Co., ForEnt Technik GmbH Co., Printing Trade Center GmbH, and Tejarat Almas Mobin Holding, for their respective roles assisting the IRGC-QF to counterfeit currency. This network used two German-based front companies to deceive European suppliers, circumvent European export restrictions, and surreptitiously procure advanced printing machinery, security printing machinery, and raw materials such as watermarked paper and specialty inks. The network used these items to print counterfeit Yemeni bank notes for the IRGC-QF. Mahmoud Seif was previously involved with the procurement of weapons for the IRGC-QF.¹³

Dual-Use Equipment Procurement for Ballistic Missile Proliferation

In February 2017, OFAC designated multiple individuals and entities that are part of the Abdollah Asgharzadeh network for the procurement of dual-use and other goods on behalf of organizations involved in Iran's ballistic missile programs. This network coordinated procurement through intermediary companies that obfuscated the final recipient of the goods. Asgharzadeh and his associates relied on a network of trusted China-based brokers and their companies to assist his procurement of dual-use and other goods.¹⁴

-
12. Shell companies are typically non-publicly traded corporations or limited liability companies (LLCs) that have no physical presence beyond a mailing address and generate little to no independent economic value. See FinCEN Guidance [FIN-2006-G014 "Potential Money Laundering Risks Related to Shell Companies"](#) (November 2006) and SAR Activity Review: [Issue 1](#) (October 2000), [Issue 2](#) (June 2001), and [Issue 7](#) (August 2004).
 13. See <https://www.treasury.gov/press-center/press-releases/Pages/sm0219.aspx>.
 14. OFAC also designated MKS International, a UAE-based company that used multiple front companies in order to circumvent export laws and sanctions to procure technology and/or materials to support Iran's ballistic missile program, as well as for acting for or on behalf of, or providing support to, Iran's IRGC-QF. See <https://www.treasury.gov/press-center/press-releases/Pages/as0004.aspx>.

Commercial Aviation Industry

Designated Iranian airlines and their agents and affiliates have used deceptive schemes to procure aviation-related materials using front companies. Treasury has issued numerous rounds of sanctions related to efforts by designated Iranian airlines to evade sanctions via the use of front or shell companies.¹⁵

Financial institutions providing services to the commercial aviation industry should be aware of prior actions by designated Iranian airlines to evade sanctions, and they are advised to exercise appropriate due diligence to ensure compliance with legal requirements. Foreign financial institutions are reminded that they may be subject to sanctions for knowingly conducting significant transactions for or with certain Iran-related persons¹⁶ (such as Mahan Air, Caspian Air, Dena Airways, Meraj Air, Pouya Air, Al-Naser Wings Airlines, Syrian Air, Khors Aircompany, Dart Airlines, and UM Air), including prohibitions or strict conditions on their ability to open or maintain correspondent or payable-through accounts in the United States. Non-U.S. persons, including foreign financial institutions, may also be subject to designation and listing on the SDN List for, e.g., providing material support to designated Iranian airlines.

Mahan Air

For many years, the Iranian Revolutionary Guards (IRGC) and other Iranian entities have transferred weapons, funds, and other items on behalf of the IRGC and provided support to the Syrian Assad regime and Lebanese Hezbollah. In 2011, OFAC designated Mahan Air for providing financial, material, and technical support to the IRGC. OFAC subsequently designated Mahan Air front companies that have violated sales contracts and obtained equipment and services for Mahan Air's aircraft in violation of U.S. sanctions. These front companies facilitate the transfer of parts, vendors, and service providers on behalf of Mahan Air, with assistance in the procurement of goods, such as aircraft parts and services from neighboring countries, Europe, and Asia. The aviation-related materials are then shipped to either the same neighboring or independent intermediary

15. For example, front companies or other companies that have been designated by OFAC for assisting designated Iranian airline Mahan Air in procuring aircraft and related parts and services include Blue Sky Aviation Co FZE; Pioneer Logistics; Asian Aviation Logistics; Avia Trust FZE; Grandeur General Trading FZE ; Aviation Capital Solutions; Aircraft, Avionics, Parts & Support Ltd.; and HSI Trading FZE. For OFAC press releases related to Mahan Air sanctions see [October 12, 2011](#); [September 19, 2012](#); [May 31, 2013](#); [February 6, 2014](#); [August 29, 2014](#); [May 21, 2015](#); [March 24, 2016](#); [September 14, 2017](#); [October 16, 2017](#); [May 24, 2018](#); and [July 9, 2018](#) at <https://home.treasury.gov/news/press-releases>.
16. These Iran-related persons include: (1) Iranian persons on the SDN List; (2) the IRGC and its designated agents or affiliates; and (3) any other person on the SDN List designated in connection with Iran's proliferation of weapons of mass destruction or their means of delivery or Iran's support for international terrorism.
17. See <https://www.treasury.gov/press-center/press-releases/Pages/j12618.aspx>, <https://www.treasury.gov/press-center/press-releases/Pages/j10395.aspx> and <https://www.treasury.gov/press-center/press-releases/Pages/j12287.aspx>.

Iran-Related Shipping Companies' Access to the Financial System

During previous periods of heightened sanctions pressure, Treasury identified Iranian or Iran-related companies using deceptive shipping practices to evade U.S. sanctions. As detailed in previous OFAC advisories and designation actions, these practices include: the use of falsified documents,²¹ the reflagging of vessels,²² and the involvement of third parties, such as brokers and trading companies, to mask the underlying payments and business activity with Iran.²³ For example, in the pre-JCPOA period, Treasury identified shipping companies around the world that falsified documents to hide ships docking in Iranian ports and the accompanying trade-related payments. In addition, in the past, as the United States has added entities or individuals to OFAC's SDN List, there have been instances where a vessel's ownership or operation was transferred from a newly-designated person to a front company or other person acting for or on behalf of the designated person.²⁴

As the sanctions on Iran that were lifted under the JCPOA come back into effect following the 90-and 180-day wind-down periods, Iranian shipping companies may return to the use of these or other evasive practices. Financial institutions may see indications of these deceptive shipping practices in the information contained in international wires, payment requests, and letters of credit. Documents may also be falsified, and include bills of lading and shipping invoices to conceal shipping routes, embarkation ports, or shipping agents. Financial institutions may find maritime databases and reports—such as those generated by the International Maritime Bureau or other available services—helpful when verifying trade-related documents.²⁵ Financial institutions should be aware of changes regarding the issuing or writing of letters of credit and other trade-related financial transactions. Financial institutions should report those changes in their SAR filings if the changes appear to be related to malign activity. In addition, among other deceptive conduct, Iranian vessels may attempt to hide their origin and purpose by potentially fabricating

21. See https://www.treasury.gov/resource-center/sanctions/Programs/Documents/20110331_advisory.pdf. In this March 31, 2011 advisory, OFAC alerted shippers, importers/exporters, and freight forwarders to practices used by the Islamic Republic of Iran Shipping Lines (IRISL), which at the time was designated pursuant to E.O. 13382, and companies acting on its behalf to evade U.S. and international economic sanctions by hiding the involvement of IRISL in shipping transactions, including (1) using container prefixes in shipping container numbers; and/or (2) omitting or listing invalid, incomplete, or false container prefixes in shipping container numbers; and/or (3) naming non-existent ocean vessels in shipping documents. See <https://www.treasury.gov/press-center/press-releases/Pages/hp1130.aspx>. IRISL and its affiliates, as well as a large number of vessels in which these entities held an interest, were removed from OFAC's SDN List on January 16, 2016 in connection with the JCPOA. No later than November 5, 2018, OFAC will reimpose, as appropriate, the sanctions that applied to persons removed from SDN List and/or other lists maintained by OFAC on January 16, 2016.
22. See https://www.treasury.gov/resource-center/sanctions/Programs/Documents/ofac_irisl_advisory_07192012.pdf. In this July 19, 2012 advisory, OFAC alerted the maritime industry that IRISL operated vessels despite their flags having been revoked. International sanctions at the time, and IRISL's efforts to evade them through deceptive practices, led to increased vigilance by the maritime industry and prompted an increasing number of countries to revoke or refuse to issue a flag to vessels in which IRISL or its affiliates had an interest. See <https://www.treasury.gov/press-center/press-releases/Pages/hp1130.aspx> and <https://www.treasury.gov/press-center/press-releases/Pages/j11933.aspx>.
23. See <https://www.treasury.gov/press-center/press-releases/Pages/TC981.aspx>.
24. See <https://www.treasury.gov/press-center/press-releases/Pages/j11933.aspx> and <https://www.treasury.gov/press-center/press-releases/Pages/TC981.aspx>.
25. See <https://www.icc-ccs.org/icc/imb>.

vessel registration and flag credentials at ports of call and canal entrances. Malign Iran-related actors and sanctioned entities engage in these activities to bypass financial institutions' SDN filters so they may evade sanctions. Financial institutions should continue to conduct appropriate due diligence to ensure they are not directly or indirectly providing services to sanctioned parties.

The Iranian Regime's Illicit Use of Precious Metals

Iran has previously used precious metals, such as gold, to evade U.S. sanctions and facilitate the sale of Iranian oil and other goods abroad. In response to these schemes, the United States enacted sanctions specifically targeting Iran's trade in precious metals, including section 1245 of the Iran Freedom and Counter-Proliferation Act of 2012. As the United States re-imposes sanctions lifted under the JCPOA, financial institutions should be aware of prior schemes used by entities with a nexus to Iran to evade sanctions using gold and other commodities.

Virtual Currency

Since 2013, Iran's use of virtual currency includes at least \$3.8 million worth of bitcoin-denominated transactions per year. While the use of virtual currency in Iran is comparatively small, virtual currency is an emerging payment system that may provide potential avenues for individuals and entities to evade sanctions. Despite public reports that the CBI has banned domestic financial institutions from handling decentralized virtual currencies, individuals and businesses in Iran can still access virtual currency platforms through the Internet. For example, virtual currency can be accessed through: (1) Iran-located, Internet-based virtual currency exchanges; (2) U.S.- or other third country-based virtual currency exchanges; and (3) peer-to-peer (P2P) exchangers.

Institutions should consider reviewing blockchain ledgers for activity that may originate or terminate in Iran. Institutions should also be aware that the international virtual currency industry is highly dynamic; new virtual currency businesses may incorporate or operate in Iran with little notice or footprint. Further, P2P exchangers—natural or legal persons who offer to buy, sell, or exchange virtual currency through online sites and in-person meetups—may offer services in Iran. These P2P exchangers may operate as unregistered foreign MSBs in jurisdictions that prohibit such businesses; where virtual currency is hard to access, such as Iran; or for the purpose of evading the prohibitions or restrictions in place against such businesses or virtual currency exchanges and other similar business in some jurisdictions. Institutions can utilize technology created to monitor open blockchains and investigate transactions to or from P2P exchange platforms.

Activity of these exchangers may involve wire transactions from many disparate accounts or locations combined with transfers to or from virtual currency exchanges. These transactions may occur when account holders fund an account or withdraw value from an account, especially if the foreign exchanger operates in multiple currencies.

Financial institutions and virtual currency providers that have BSA and U.S. sanctions obligations should be aware of and have the appropriate systems to comply with all relevant sanctions requirements and AML/CFT obligations. Sanctions requirements may include not only screening

against the SDN List but also appropriate steps to comply with other OFAC-administered sanctions programs, including those that impose import and/or export restrictions with respect to particular jurisdictions.²⁶ Further, a non-U.S.-based exchanger or virtual currency provider doing substantial business in the United States is subject to AML/CFT obligations and OFAC jurisdiction.

U.S. individuals and institutions involved in virtual currency should be aware of OFAC's March 2018 Frequently Asked Questions (FAQs) on sanctions issues associated with virtual currencies.²⁷ The FAQs remind U.S. persons that their compliance obligations with respect to transactions are the same, regardless of whether a transaction is denominated in virtual currency or not. OFAC also states as a general matter that U.S. persons and persons otherwise subject to OFAC jurisdiction, including firms subject to OFAC jurisdiction that facilitate or engage in online commerce or process transactions using "digital currency," are responsible for ensuring that they do not engage in unauthorized transactions prohibited by OFAC sanctions, such as dealings with blocked persons or property, or engaging in prohibited trade or investment-related transactions.²⁸ Prohibited transactions include transactions that evade or avoid, have the purpose of evading or avoiding, cause a violation of, or attempt to violate prohibitions imposed by OFAC under various sanctions authorities. Additionally, persons that provide financial, material, or technological support for or to a designated person may be designated by OFAC under the relevant sanctions authority.²⁹

Financial Action Task Force's Findings Related to Iran's Anti-Money Laundering/Combating the Financing of Terrorism Regime

The Financial Action Task Force (FATF) has listed Iran as a jurisdiction with systemic deficiencies in its AML/CFT regime. Despite Iran's commitment in June 2016 to an action plan with the FATF to address its AML/CFT deficiencies, Iran has failed to complete the majority of its action plan. The FATF therefore continues to call upon its members and all jurisdictions to advise their financial institutions to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons from Iran.

In addition to keeping Iran on its Public Statement, on June 29, 2018, the FATF expressed disappointment with Iran's failure to implement its action plan, and it reiterated its concern with the terrorist financing risk emanating from Iran and the threat this poses to the international financial system. The FATF noted that Iran "should fully address its remaining action items, including by: (1) adequately criminalising terrorist financing, including by removing the exemption for designated groups 'attempting to end foreign occupation, colonialism and racism'; (2) identifying and freezing terrorist assets in line with the relevant United Nations Security Council

26. If a financial institution or virtual currency provider has questions concerning OFAC sanctions, they can either call OFAC's Toll-Free Hotline at 1-800-540-6322, or email OFAC's Feedback Account at OFAC_Feedback@treasury.gov.

27. See FAQ 559 to 563, available at https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx.

28. For the purposes of OFAC sanctions programs, the term "digital currency" includes digital fiat currency or sovereign cryptocurrency, virtual currency (non-fiat), and digital representations of fiat currency.

29. See FAQ 560, available at https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx.

resolutions; (3) ensuring an adequate and enforceable customer due diligence regime; (4) ensuring the full independence of the Financial Intelligence Unit and requiring the submission of STRs [Suspicious Transaction Reports] for attempted transactions; (5) demonstrating how authorities are identifying and sanctioning unlicensed money/value transfer service providers; (6) ratifying and implementing the Palermo and TF [Terrorist Financing] Conventions and clarifying the capability to provide mutual legal assistance; (7) ensuring that financial institutions verify that wire transfers contain complete originator and beneficiary information; (8) establishing a broader range of penalties for violations of the ML [Money Laundering] offense; and (9) ensuring adequate legislation and procedures to provide for confiscation of property of corresponding.³⁰ The FATF will decide upon the appropriate action in October 2018 if Iran has not by then enacted the necessary amendments to its AML and CFT laws and ratified the Terrorist Financing and Palermo Conventions. All available advisories on FATF Plenaries, including previous years, are available at <https://www.fincen.gov/resources/advisoriesbulletinsfact-sheets/advisories>.

Red Flags Related to Deceptive Iranian Activity

The following red flags may help financial institutions identify suspicious activity involving the schemes discussed above. In applying these red flags, financial institutions are advised that no single transactional red flag necessarily indicates suspicious activity, and institutions should ensure that their assessments are in line with their internal risk profile. Financial institutions should consider additional indicators and the surrounding facts and circumstances, such as a customer's historical financial activity and the existence of other red flags, before determining that a transaction is suspicious. Financial institutions should also perform additional inquiries and investigations where appropriate. Foreign financial institutions may find the information beneficial for their risk and threat assessments and suspicious transaction reporting requirements. The appropriate financial crimes compliance/sanctions compliance within the financial institution should be apprised of any transactions that are determined to involve Iran.

Illicit Activity by the CBI or Its Officials

Use of Personal Account. The CBI or CBI officials route transactions to personal accounts instead of central bank or government-owned accounts. Individuals or entities with no central bank or government affiliation withdraw funds from such accounts.

Unusual Wire Transfers. The CBI engages in multiple wire transfers to banks or financial institutions that the CBI would not normally engage in, or that are not related to traditional central bank activity.³¹

30. See <http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/public-statement-june-2018.html>.

31. Effective November 5, 2018, foreign financial institutions will be subject to correspondent or payable-through account sanctions for conducting or facilitating certain significant financial transactions with the CBI, pursuant to section 1245 of the National Defense Authorization Act for Fiscal Year 2012 (NDAA).

- 3 **Use of Forged Documents.** Front companies acting for or on behalf of designated persons use forged documents to conceal the identity of parties involved in the transactions. For example, as a part of the IRGC-QF's currency exchange network scheme, documents were forged by an IRGC-QF front company manager to mislead authorities and conceal the true customers of the entities involved in the scheme.

Illicit Activity through Exchange Houses

- 4 **Use of Multiple Exchange Houses.** Customers may have transactions moving through multiple exchange houses, adding additional fees and costs as they progress through the system. The fees, number of transactions, and patterns of transactions are atypical to standard and customary commercial practices.
- 5 **Multiple Depositors.** Account holders that receive deposits—that do not appear to match the customer's profile or provided documentation—from numerous individuals and entities.

Use of Procurement Networks

- 6 **Shell or Front Companies.** Transactions involving companies that originate with, or are directed to, entities that are shell corporations, general "trading companies", or companies that have a nexus with Iran. For example, a company has an affiliate in Iran or is owned by individuals known to be loyal to the Iranian regime, and appears to lack a general business purpose. Iran uses front companies incorporated across the world, including in Asia and Europe. Other indicators of possible shell companies include opaque ownership structures, individuals/entities with obscure names that direct the company, or business addresses that are residential or co-located with other companies.
- 7 **Suspicious Declarations.** Declarations of information that are inconsistent with other information, such as previous transaction history or nature of business. Declarations of goods that are inconsistent with the associated transactional information.
- 8 **Unrelated Business.** Transactions that are directed to companies that operate in unrelated businesses, and which do not seem to comport with the Customer Due Diligence (CDD) and other customer identification information collected during client onboarding and subsequent refreshes.

Illicit Procurement of Aircraft Parts

- 9 **Use of Front Companies and Transshipment Hubs to Source Aircraft Parts.** Financial institutions that facilitate commercial aviation-related financial transactions where the beneficial ownership of the counterparty is unknown and the delivery destination is a common transshipment point for onward delivery to Iran. Iran-linked persons have attempted to source U.S.-origin aircraft and related parts from third countries known to be hubs for maintenance, repair, and overhaul operations, and then use front companies located in third-countries to conceal or obfuscate the ultimate Iranian beneficiary of the U.S.-origin aircraft, parts, and aviation-related materials.

- 10** *Misrepresentation of Sanctions.* Misrepresenting to suppliers, dealers, brokers, re-insurers, and other intermediaries that sanctions against Iran have been lifted or are no longer applicable as a result of the JCPOA, or falsely claiming without supporting documentation that an OFAC license has been obtained.

Iran-Related Shipping Companies' Access to the U.S. Financial System

- 11** *Incomplete and Falsified Documentation.* Transactions and wire transfers that include bills of lading with no consignees or involving vessels that have been previously linked to suspicious financial activities. Documentation, such as bills of lading and shipping invoices, submitted with wire and payment requests that may appear to be falsified, or with key information omitted, in an attempt to hide the Iranian nexus.
- 12** *Inconsistent Documentation for Vessels Using Key Ports.* Inconsistencies between shipping-related documents and maritime database entries that are used for conducting due diligence. For example, the maritime database may indicate that a vessel docked in an Iranian port, even though this information is not included in the shipping documents submitted to financial institutions for payment processing. Major ports in Iran are Bandar Abbas, Assaluyeh, and Bandar-e Emam Khomeyni, which is also known as Abadan. Port cities on the Gulf include: Ahvaz, Bushehr, Bandar-e Lengeh, Bandar-e Mahshahr, Chabahar, Kharg Island, and Lavan Island. Kharg Island and Lavan Island are major oil and gas ports.
- 13** *Previous Ship Registration to Sanctioned Entities.* Vessels whose ownership or operation is transferred to another person—following OFAC's designation of its owner or operator—on behalf of the designated person, but the designated owner or operator maintains an interest in the vessel.

Suspicious Funds Transfers

- 14** *Lack of Information Regarding Origin of Funds.* Wire transfers or deposits that do not contain any information about the source of funds, contain incomplete information about the source of funds, or do not match the customer's line of business.
- 15** *Unusual or Unexplainable Wire Transfers.* Multiple, unexplained wire transfers and transfers that have no apparent connection to a customer's profile. For example, individuals may claim that the unusually high-value wire transfers they receive from one or more foreign countries are merely funds sent from relatives in Iran. In addition, wire transfers to accounts in the United States from high-risk jurisdictions that have no apparent connection to the customer's line of business.

FINCEN ADVISORY

- 16** *Using Funnel Accounts.* Third parties from across the United States who deposit funds into the accounts of U.S.-based individuals with ties to Iran.³² The deposits and associated transactions do not match the account holder's normal geographical footprint, and the source of the funds is unknown or unclear.
- 17** *Structuring Transactions.* U.S. persons send or receive money to or from Iran by structuring the cash portion of the transactions to avoid the currency transaction reporting threshold of \$10,000. Individuals returning to the United States from Iran also may make large deposits of monetary instruments rather than cash.
- 18** *Gold.* Given Iran's prior use of gold as a substitute for cash to evade U.S. sanctions, financial institutions should consider conducting additional due diligence on transactions related to precious metals, particularly in geographic regions in close proximity to Iran (such as Turkey) that engage in significant gold-related transactions. Additionally, financial institutions may notice transactions not obviously linked to Iran, but related to the purchase of unusually high volumes of gold.

Virtual Currency

- 19** *Logins from Iranian Internet Protocol Addresses or with Iranian Email.* Internet Protocol (IP) login activity from entities in Iran or using an Iranian email service in order to transact virtual currencies through a virtual currency exchange. In such cases, financial institutions may also be able to provide associated technical details such as IP addresses with time stamps, device identifiers, and indicators of compromise that can provide helpful information to authorities.³³
- 20** *Payments to/from Iranian Virtual Currency Entity.* A customer or correspondent payment to or from virtual currency exchanges that appear to be operating in Iran.
- 21** *Peer-to-Peer (P2P) Exchangers.* Unexplained transfers into a customer account from multiple individual customers combined with transfers to or from virtual currency exchanges. Wire transfers are usually associated with funding an account or withdrawing value, especially with foreign exchanges that may operate in multiple currencies.

32. Funnel account activity often involves a customer structuring currency deposits into an account in one geographic area, with the funds subsequently withdrawn in a different geographic region with little time elapsing between deposit and withdrawal. The rapid flow of funds may also span a large geographic area between the deposits and withdrawals, including instances where the deposit location is thousands of miles away from the withdrawal location. In some instances, these disparate deposits have been consolidated into a single account and withdrawn from the consolidated account. The currency deposits and withdrawals often have no apparent lawful or business purpose and do not reflect the stated occupation of the account holder. For a detailed description of funnel accounts, see <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2012-a006> and <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2014-a005>.

33. See Question #1 in "FAQs regarding the Reporting Cyber-Events, Cyber-Enabled Crime, and Cyber-Related Information through SARs" (October 2016) as well as "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime," available at: [https://www.fincen.gov/sites/default/files/shared/FAQ Cyber Threats 508 FINAL.PDF](https://www.fincen.gov/sites/default/files/shared/FAQ%20Cyber%20Threats%20508%20FINAL.PDF) and [https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508 2.pdf](https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508%202.pdf).

FINCEN ADVISORY

FinCEN expects that Iranian financial institutions, the Iranian regime, and its officials will increase their efforts to evade U.S. sanctions to fund malign activities and secure hard currency for the Government of Iran, following the re-imposition of sanctions lifted under the JCPOA. Treasury and the U.S. Government are interested in information related to Iran's efforts outlined in this advisory, as well as information pertaining to how Iran or Iranian entities subject to sanctions, including the CBI, otherwise evade the sanctions and access the U.S. financial system.

This advisory does not describe all of the methods the Government of Iran may use to gain access to the U.S. financial system or evade sanctions, such as using funnel accounts or informal value transfer systems (IVTS).³⁴ FinCEN encourages financial institutions to review past advisories relating to Iran, including FinCEN Advisory FIN-2018-A004 "Advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies" (September 2018),³⁵ FinCEN Advisory FIN-2010-A008 "Update on the Continuing Illicit Finance Threat Emanating from Iran" (June 2010),³⁶ FinCEN Advisory FIN-2008-A002 "Guidance to Financial Institutions on the Continuing Money Laundering Threat Involving Illicit Iranian Activity" (March 2008),³⁷ and FinCEN Advisory FIN-2007-A001 "Guidance to Financial Institutions on the Increasing Money Laundering Threat Involving Illicit Iranian Activity" (October 2007).³⁸

U.S. Sanctions

U.S. primary sanctions on Iran are those sanctions administered by OFAC that broadly prohibit U.S. persons and U.S.-owned or -controlled organizations from engaging in virtually all transactions or dealings with or on behalf of the Government of Iran or Iranian financial institutions, unless the transactions are specifically authorized or expressly authorized by the U.S. Government.³⁹ These prohibitions also apply to transactions in Iran that are conducted through the United States, as well as other types of activities, such as certain types of Iranian transactions and sanctions regulations. OFAC prohibits the exportation of goods, services (including financial services) or technology directly or indirectly from the United States or by a U.S. person to Iran. Pursuant to this provision, U.S. financial institutions are prohibited from opening or maintaining correspondent accounts for, or being owned or controlled by, Iranian financial institutions. A general exemption of OFAC authorizes U.S. financial institutions, including foreign branches and subsidiaries, to process transactions for or through the United States in violation of this provision, including transactions through U.S. correspondent accounts, for or on behalf of Iranian financial institutions, other Iranian persons, or where the benefits otherwise received in Iran.

34. The term Informal Value Transfer System (IVTS), as originally stated in the March 2003 "IVTS Advisory," refers to any system, mechanism, or network of people that receives money for the purpose of making the funds or an equivalent value payable to a third party in another geographic location, whether or not in the same form. See <https://www.fincen.gov/sites/default/files/shared/advis33.pdf>.

35. See <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2018-a004>.

36. See <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2010-a008>.

37. See <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2008-a002>.

38. See <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2007-a001>.

39. See Iranian Transactions and Sanctions Regulations, 31 CFR Part 560.

FINCEN ADVISORY

The laws of the United States apply to all persons, whether or not owned or controlled by the Government of a foreign country, except from violation or expression authorized by the U.S. Government. There are often prohibitions on providing support to U.S. persons in such a way as to circumvent or evade U.S. sanctions.

U.S. persons are also subject to local prohibitions on dealings with and must block the property and interests in property of such persons, and related persons, designated pursuant to executive orders, specifically E.O. 13339 and E.O. 13382, and prohibitions on transfer of weapons of mass destruction or their means of delivery, and related persons. All human financial transactions are blocked under Executive Order 13339 and section 50111 of the WSR and E.O. 13382, except for CIA and certain U.S. persons involved in the property and interests in property of all human threats. (AS 11/10/11)

Pursuant to the International Sanctions Regulations (ISRs) and multiple secondary and executive orders, U.S. financial institutions, and persons subject to sanctions for knowingly conducting certain transactions for or with certain international persons including preparations or other activities of their ability to open, maintain, cross-border, or payable through accounts in the United States, various persons, including foreign financial institutions, may also be subject to blocking sanctions by U.S. persons, including U.S. persons designated persons. U.S. financial institutions should be advised of their obligations under OFAC sanctions to prevent any use of their accounts and other U.S. financial system accounts for transactions involving an Iranian financial institution. OFAC has issued guidance to U.S. financial institutions and persons to prohibit transactions involving U.S. financial system that involve Iranian financial institutions, including U.S. financial institutions and persons, including certain financial institutions. As a result, the industry should continue to develop controls designed to detect and prevent involvement of Iranian banks or financial institutions through other means involving the U.S. financial system. In many cases, the requirements for financial institutions to comply with Iran Country E.O. 13382 and E.O. 13339, and other U.S. financial system controls, may be more stringent than those implemented by U.S. financial institutions. U.S. financial institutions should continue to monitor and maintain levels of screening and review for transactions originating from or otherwise involving institutions in close proximity to Iran. Financial institutions engaged in these border wire transfer should be aware of the factors involving sanctions, with varying geographic and economic restrictions. These practices generally result in significant oversight of cross-border accounts, including wire transfers, as well as create an early high degree of scrutiny related to payments and funds transfers originating from or to Iran, Iraq, Cuba, and entities.

Additional information on these sanctions, including sanctions that are being imposed following the withdrawal of the United States from the JCPOA, can be found at <http://www.treasury.gov/press-center/press-releases/Pages/20180801>.

40. See, e.g., E.O. 13224 and the Global Terrorism Sanctions Regulations, 31 CFR Part 594; E.O. 13382 and the Weapons of Mass Destruction Proliferators Sanctions Regulations; and E.O. 13553 and the Iranian Human Rights Abuses Sanctions Regulations, 31 CFR Part 562.

Reminder of Regulatory Obligations for U.S. Financial Institutions

Consistent with existing regulatory obligations, U.S. financial institutions should take reasonable and prudent steps to determine and maintain an effective BSA policy to funds and other assets associated with individuals and entities involved in laundering their interests, including those associated with sanctions evasion.

Reminder of AML and Regulatory Obligations for U.S. Financial Institutions Regarding Due Diligence, Correspondent Accounts, CISADA, and Suspicious Activity Reporting

FINCEN is providing the information in this advisory to assist U.S. financial institutions in meeting their risk-based due diligence obligations and to inform entity beneficial owners who are providing financial information on behalf of sanctioned individuals and entities.

Enhanced Due Diligence Obligations for Private Banking Accounts

In addition to the general risk-based due diligence obligations under section 312 of the USA PATRIOT Act (31 U.S.C. 3121) and its implementing regulations, U.S. financial institutions have regulatory obligations to implement an enhanced due diligence program for private banking accounts held for non-U.S. persons that is designed to detect and report any known or suspected money laundering or other suspicious activity.

Corporate Due Diligence and Identification of Beneficial Owners of New Legal Entity Accounts

As of May 11, 2018, FINCEN's CDB Rule requires banks, brokers or dealers in securities, mutual funds and futures commission members, and introducing brokers in commodities to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions.⁴¹ This rule includes the identification of legal entities that may be owned or controlled by individuals and entities reported by the relevant reporting

41. See 31 CFR § 1010.620(a-b). The definition of "covered financial institution" is found in 31 CFR § 1010.605(e). The definition of "private banking account" is found in 31 CFR § 1010.605(m). The definition of "non-U.S. person" is found in 31 CFR § 1010.605(h).

42. See 31 CFR § 1010.230 (describing beneficial ownership requirements for legal entity customers).

FINCEN ADVISORY

General Obligations for Correspondent Accounts, Due Diligence and Anti-Money Laundering Programs

U.S. financial services providers are required to comply with their general due diligence obligations under 31 CFR § 1010.210, in addition to the general AML program obligations under 31 CFR § 1010.210 and its implementing regulations. As required under 31 CFR § 1010.210, covered financial institutions must establish and maintain due diligence programs which address correspondent relationships and monitor for foreign financial institutions which appropriate specific risk-based due diligence procedures, procedures, and controls that are reasonably designed to detect and report from or suspected money laundering activity conducted through correspondent or non-correspondent accounts established, maintained, administered, or managed within the United States.

Comprehensive Sanctions, Accountability, and Deterrence Act of 2010

FINCEN also reminds U.S. banks of the reporting requirements provided with *Comprehensive Sanctions, Accountability, and Deterrence Act of 2010* (CSDA) under 31 CFR 1010.210. Banks must report to FINCEN, as a matter of a specified foreign bank for which it maintains correspondent accounts, or through which it has processed the following: membership foreign bank numbers a correspondent account, or through which it has processed transfers of funds on behalf of a foreign bank financial institution designated under the International Emergency Economic Powers Act (IEEPA), and where the foreign bank has processed transfers of funds for the IEEPA or any of its agents or affiliates designated under IEEPA.

Suspicious Activity Reporting

A financial institution may be required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity, or attempts to derive funds from illegal activity, is designed to evade regulations promulgated under the BSA, lacks a business or apparent lawful purpose, or involves the use of the proceeds of a crime or other unlawful activity which may constitute a violation of the law.

43. See 31 CFR § 1010.210 (regarding anti-money laundering program requirements).

44. See 31 CFR § 1060.300(a).

45. See generally 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320

FINCEN ADVISORY

SAR Filing Instructions

When filing a SAR, financial institutions should provide all possible available information in the SAR form and narrative. FinCEN further requests that financial institutions reference this advisory by including the key term:

“(FinCEN 2015-006)”

to indicate a connection between the suspicious activity being reported and the narrative and activities highlighted in this advisory.

For Further Information

Additional questions or comments regarding the contents of this advisory should be addressed to the FinCEN Resource Center at FRC@fincen.gov.

Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day). The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

Financial institutions or virtual currency providers having questions concerning OFAC sanctions should either call OFAC's Toll-Free Hotline at 1-800-540-6322, or email OFAC's Feedback Account at OFAC_Feedback@treasury.gov.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.

ΠΑΡΑΡΤΗΜΑ VI

Επικαιροποίηση της νομοθεσίας θωράκισης για τη στήριξη της συμφωνίας με το Ιράν για τα πυρηνικά

Καθώς στις 7 Αυγούστου 2018 άρχισε να ισχύει η πρώτη δέσμη κυρώσεων των ΗΠΑ που επιβλήθηκαν εκ νέου κατά του Ιράν, τέθηκε παράλληλα σε ισχύ η επικαιροποιημένη νομοθεσία θωράκισης της ΕΕ, ούτως ώστε να μετριαστούν οι επιπτώσεις των εν λόγω κυρώσεων για τα συμφέροντα των ευρωπαϊκών επιχειρήσεων που ασκούν νόμιμες επιχειρηματικές δραστηριότητες στο Ιράν.

Η επικαιροποιημένη νομοθεσία θωράκισης αποτελεί μέρος της στήριξης που παρέχει η Ευρωπαϊκή Ένωση για τη συνέχιση της πλήρους και αποτελεσματικής εφαρμογής του Κοινού Ολοκληρωμένου Σχεδίου Δράσης (ΚΟΣΔ), δηλαδή της συμφωνίας με το Ιράν για τα πυρηνικά, μεταξύ άλλων μέσω της στήριξης του εμπορίου και των οικονομικών σχέσεων μεταξύ της ΕΕ και του Ιράν, οι οποίες εξομαλύνθηκαν μετά την άρση των κυρώσεων ως αποτέλεσμα του ΚΟΣΔ.

Η διαδικασία επικαιροποίησης της νομοθεσίας θωράκισης κινήθηκε από την Επιτροπή στις 6 Ιουνίου 2018, και συνίσταται στην προσθήκη, στο πεδίο εφαρμογής της σχετικής νομοθετικής πράξης, των εξωεδαφικών κυρώσεων τις οποίες επιβάλλουν εκ νέου οι ΗΠΑ στο Ιράν. Ακολούθησε περίοδος ελέγχου δύο μηνών από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο. Καθώς δεν διατυπώθηκε καμία αντίρρηση, η επικαιροποίηση δημοσιεύθηκε και τέθηκε σε ισχύ στις 7 Αυγούστου 2018.

Η νομοθεσία θωράκισης επιτρέπει στους οικονομικούς φορείς της ΕΕ να αποζημιώνονται, από τα πρόσωπα που τις προκαλούν, για ζημιές που προκύπτουν από εξωεδαφικές κυρώσεις που εμπίπτουν στο πεδίο εφαρμογής της και ακυρώνει τα αποτελέσματα στην ΕΕ των αλλοδαπών δικαστικών αποφάσεων που βασίζονται σε αυτές τις κυρώσεις. Επίσης, απαγορεύει σε φυσικά και νομικά πρόσωπα της ΕΕ να συμμορφώνονται με τις εν λόγω κυρώσεις, εκτός εάν λάβουν κατ' εξαίρεση άδεια από την Επιτροπή, σε περίπτωση που η μη συμμόρφωσή τους βλάπτει σοβαρά τα συμφέροντά τους ή τα συμφέροντα της Ένωσης.

Για να υποστηριχθούν οι οικονομικοί φορείς της ΕΕ κατά την εφαρμογή της επικαιροποιημένης νομοθεσίας θωράκισης, η Επιτροπή εξέδωσε επεξηγηματικό σημείωμα για να διευκολύνει την κατανόηση των σχετικών νομικών πράξεων.

Ένα υπόδειγμα είναι στη διάθεση των οικονομικών φορέων της ΕΕ που θεωρούν ότι η μη συμμόρφωση με τη σχετική εξωεδαφική νομοθεσία που εμπίπτει στο πεδίο εφαρμογής της νομοθεσίας θωράκισης θα έθιγε σοβαρά τα συμφέροντά τους ή τα συμφέροντα της Ένωσης, προκειμένου να τους βοηθήσει να προετοιμαστούν και να υποβάλουν αίτηση για τη χορήγηση άδειας. Η δυνατότητα υποβολής αίτησης για άδεια προβλέπεται ως εξαίρεση στον κανονισμό (ΕΚ) αριθ. 2271/96, χωρίς αυτό να δημιουργεί ατομικό δικαίωμα για τον αιτούντα όσον αφορά τη χορήγηση άδειας. Η Επιτροπή θα αξιολογεί κάθε αίτηση και θα χορηγεί στον αιτούντα συνοπτική αιτιολογημένη απόφαση. Οι αιτήσεις θα αξιολογούνται βάσει συμφωνημένων κριτηρίων, τα οποία επίσης εκδόθηκαν στις 7 Αυγούστου 2018.

Επιπλέον, οι οικονομικοί φορείς της ΕΕ θα πρέπει να λαμβάνουν υπόψη ότι δεν θα πρέπει να χρησιμοποιούν τη διαδικασία αδειοδότησης επιδιώκοντας τη διατύπωση από την Επιτροπή «δηλώσεων προθέσεων» ή βεβαίωσης ότι οι επιχειρηματικές τους αποφάσεις συνάδουν με τη νομοθεσία θωράκισης.

Στη σελίδα αυτή θα βρείτε τα σχετικά έγγραφα που σχετίζονται με τη νομοθεσία θωράκισης: ο κανονισμός, όπως εκδόθηκε το 1996, οι νομικές πράξεις που τέθηκαν σε ισχύ στις 7 Αυγούστου 2018 (εκτελεστικός κανονισμός της Επιτροπής και κατ' εξουσιοδότηση πράξη για την επικαιροποίηση της νομοθεσίας θωράκισης), το επεξηγηματικό σημείωμα που θα σας βοηθήσει να κατανοήσετε καλύτερα αυτές τις διατάξεις, καθώς και υπόδειγμα για την εξέταση και την υποβολή τυχόν αίτησης για κατ' εξαίρεση χορήγηση άδειας από την Επιτροπή για τη συμμόρφωση προς τη σχετική εξωεδαφική νομοθεσία που εμπίπτει στο πεδίο εφαρμογής της νομοθεσίας θωράκισης, σε περίπτωση που η μη συμμόρφωση θα έθιγε σοβαρά τα συμφέροντά σας ή τα συμφέροντα της Ένωσης.

Κατάλογος εγγράφων

- [Κανονισμός \(ΕΚ\) αριθ. 2271/96 του Συμβουλίου, της 22ας Νοεμβρίου 1996, για την προστασία από τις συνέπειες της εξωεδαφικής εφαρμογής ορισμένων νόμων](#)

<https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:01996R2271-20140220> (EL)

- [Κατ' εξουσιοδότηση κανονισμός \(ΕΕ\) 2018/1100 της ΕΠΙΤΡΟΠΗΣ, της 6.6.2018, για την τροποποίηση του παραρτήματος του κανονισμού \(ΕΚ\) αριθ. 2271/96 του Συμβουλίου, της 22ας Νοεμβρίου 1996, για την προστασία από τις συνέπειες της εξωεδαφικής εφαρμογής ορισμένων νόμων που θεσπίστηκαν από μια τρίτη χώρα, και των μέτρων που βασίζονται σε αυτούς ή απορρέουν από αυτούς](#)

<https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32018R1100> (EL)

- [Εκτελεστικός κανονισμός \(ΕΕ\) 2018/1101 της Επιτροπής για τον καθορισμό των κριτηρίων εφαρμογής του δεύτερου εδαφίου του άρθρου 5 του κανονισμού \(ΕΚ\) αριθ. 2271/96 του Συμβουλίου, της 22ας Νοεμβρίου 1996, για την προστασία από τις συνέπειες της εξωεδαφικής εφαρμογής ορισμένων νόμων που θεσπίστηκαν από μια τρίτη χώρα, και των μέτρων που βασίζονται σ' αυτούς ή απορρέουν από αυτούς](#)

<https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32018R1101> (EL)

- [Επεξηγηματικό σημείωμα: Ερωτήσεις και απαντήσεις: έγκριση της επικαιροποίησης της νομοθεσίας θωράκισης](#)

[https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:52018XC0807\(01\)](https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:52018XC0807(01)) (EL)

- [Υπόδειγμα αιτήσεων χορήγησης αδειών βάσει του άρθρου 5 δεύτερο εδάφιο του κανονισμού \(ΕΚ\) αριθ. 2271/96 του Συμβουλίου, για την προστασία από τις συνέπειες της εξωεδαφικής εφαρμογής ορισμένων νόμων που θεσπίστηκαν από μια τρίτη χώρα, και των μέτρων που βασίζονται σ' αυτούς ή απορρέουν από αυτούς \(ο «κανονισμός»\)](#)

Πηγή: ιστοσελίδα Ευρωπαϊκής Επιτροπής:

http://ec.europa.eu/dgs/fpi/what-we-do/blocking_statute_en.htm

ΠΑΡΑΡΤΗΜΑ V

Joint statement by High Representative Federica Mogherini and Foreign Ministers Jean-Yves Le Drian of France, Heiko Maas of Germany and Foreign Secretary Jeremy Hunt of the United Kingdom and Finance Ministers Bruno Le Maire of France, Olaf Scholz of Germany and Philip Hammond of the United Kingdom

02/11/2018

We deeply regret the further re-imposition of sanctions by the United States, due to the latter's withdrawal from the Joint Comprehensive Plan of Action (JCPoA).

The JCPoA is a key element of the global nuclear non-proliferation architecture and of multilateral diplomacy, endorsed unanimously by the UN Security Council through Resolution 2231. It is crucial for the security of Europe, the region, and the entire world.

The JCPoA is working and delivering on its goal. The International Atomic Energy Agency (IAEA) has confirmed in twelve consecutive reports that Iran is abiding by its commitments under the Agreement.

We expect Iran to continue implementing all its nuclear commitments in full, as set out by the JCPoA.

The JCPoA also provides for the lifting of international sanctions in order to have a positive impact on trade and economic relations with Iran, but most importantly on the lives of the Iranian people.

It is our aim to protect European economic operators engaged in legitimate business with Iran, in accordance with EU law and with UN Security Council resolution 2231.

As parties to the JCPoA, we have committed to work on, inter alia, the preservation and maintenance of effective financial channels with Iran, and the continuation of Iran's export of oil and gas. On these, as on other topics, our work continues, including with Russia and China as participants to the JCPoA and with third countries interested in supporting the JCPoA. These efforts have been intensified in recent weeks, particularly those underpinning the European initiative to establish a Special Purpose Vehicle on which we are proceeding with work to set up. This will enable continued sanctions lifting to reach Iran and allow for European exporters and importers to pursue legitimate trade.

Further work must be done to assist and reassure economic operators pursuing legitimate business under EU law. Our Finance Ministers will further pursue this at their next meeting. Our collective resolve to complete this work is unwavering.

We remain committed to implementing the JCPoA as a matter of respecting international agreements and of our shared international security, and expect Iran to play a constructive role in this regard.