Expanding The Extraterritorial Reach Of US Sanctions

Law360, New York (May 14, 2012, 1:19 PM ET) -- In less than a two-week period, President Obama issued two executive orders expanding sanctions against Iran and Syria administered by the U.S. Treasury Department’s Office of Foreign Assets Control. These important new sanctions focus, respectively, on “cyber-suppression” and “foreign sanctions evaders,” and both reflect the administration’s increased willingness to target third-country nationals that engage in a wide array of activities involving Iran or Syria.

In addition, these increased measures serve to demonstrate the expanding extraterritorial reach of U.S. sanctions against Iran and Syria, even for activities without any connection to U.S. commerce and that otherwise would be lawful in the home jurisdictions of such third-country nationals.

Cyber-Suppression

On April 23, 2012, President Obama issued Executive Order 13606. The so-called “GHRAVITY E.O.” (for “Grave Human Rights Abuses by the Governments of Iran and Syria Via Information Technology”) blocks the property, and bans entry into the United States, of persons who engage in the following activities associated with computer or network disruption, monitoring, or tracking that could assist in or enable human rights abuses on behalf of the Iranian or Syrian governments (“cyber-suppression”):

- operating, or directing the operation of, information and communications technology that facilitates cyber-suppression;
- selling, leasing, or otherwise providing, directly or indirectly, goods, services, or technology to Iran and Syria likely to be used to facilitate cyber-suppression; or
- materially assisting, sponsoring, or providing financial, material, or technological support for, or goods or services to or in support of, cyber-suppression or persons designated under the GHRAVITY E.O.

The GHRAVITY E.O. explicitly designates for sanctions several Iranian and Syrian governmental entities and telecommunications companies, as well as the director of the Syrian General Intelligence Directorate. It also applies to persons owned or controlled by, or acting for or on behalf of, directly or indirectly, any person designated under the order. In addition, it potentially targets, through future designation by the secretary of the treasury, anyone else who engages in the aforementioned activities.
Currently, U.S. persons are prohibited from engaging in the cyber-suppression activities described in the executive order under existing sanctions. But the GHRAVITY E.O. threatens also to punish, among others, non-U.S. companies deemed to have engaged in these activities. This presents acute risks, for example, for non-U.S. companies that may be engaged in activities that are lawful within their home jurisdictions but now sanctionable under the GHRAVITY E.O.

Non-U.S. companies (and individuals) now face the prospect of having their assets blocked, effectively denying them access to the U.S. commercial and financial sectors. In addition, designated individuals could be barred from entry into the United States.

The language of the GHRAVITY E.O. is, by design, expansive and ambiguous. To better achieve the goal of curtailing Internet censorship and electronic surveillance in Iran and Syria, it seems likely that the administration intends the GHRAVITY E.O. to have a general in terrorem effect on non-U.S. actors who persist in dealing with those countries by extending the threat of direct U.S. sanctions to their wholly extraterritorial activities. However, with no standard of knowledge articulated, it is unclear how non-U.S. persons will recognize, for example, if their activities indirectly facilitate or support cyber-suppression as sweepingly described by the order.

Foreign Sanctions Evaders

Approximately one week after the GHRAVITY E.O. was issued, the administration issued Executive Order 13608, targeting “foreign sanctions evaders” ("FSEs") with respect to Iran and Syria (the “FSE E.O.”). The FSE E.O. empowers OFAC to impose sanctions against non-U.S. persons who are found to have “violated, attempted to violate, conspired to violate or caused a violation of any license, order, regulation, or prohibition contained in, or issued pursuant to” other executive orders that form the foundation for OFAC's sanctions programs against Iran and Syria.

The FSE E.O. also authorizes OFAC to impose sanctions against non-U.S. persons who have “facilitated deceptive transactions for or on behalf of” persons subject to U.S. sanctions against Iran and Syria, and on non-U.S. persons owned or controlled by, or acting on behalf of, directly or indirectly, designated FSEs. As defined in the FSE E.O., a “deceptive transaction” is one in which the identity of an Iranian or Syrian sanctions target is withheld or obscured from other parties or relevant regulatory authorities (e.g., non-U.S. export licensing officials).

The FSE E.O. prohibits all direct or indirect transactions or dealings with FSEs involving the exportation, re-exportation, or importation of goods, services, or technology to or from the United States (including U.S. financial services, broadly construed). Like the GHRAVITY E.O., the FSE E.O. bars entry into the United States of individual FSEs. Unlike the GHRAVITY E.O., the FSE E.O. does not block FSE property. But the transaction ban effectively denies FSEs access to the U.S. commercial and financial sectors, and U.S. persons are prohibited from dealing with FSEs in any activity involving goods, services, or technology leaving or entering the United States.

In addition, while U.S. banks are not required to block FSE property in their control or custody, they are prohibited (absent a license from OFAC) from operating FSE accounts on their books, and must reject and report to OFAC any attempted financial transactions prohibited under the FSE E.O.
OFAC has not yet named any FSEs subject to these sanctions.

**Extraterritoriality Plus Ambiguity Equals Heightened Risks for Non-U.S. Companies**

These two new executive orders apply different sanctions (i.e., blocking measures versus prohibitions on transactions) to achieve essentially the same result; i.e., to deny access to U.S. commerce to third-country parties whose conduct in some way undermines U.S. sanctions against Iran and Syria. Although the GHRAVITY E.O. also directly targets Iranian and Syrian governmental and commercial entities, both executive orders bring to bear the full power of U.S. economic sanctions on non-U.S. persons in third countries engaged in activity wholly outside of U.S. commerce.

Compounding the risks — especially for non-U.S. companies engaged in activities otherwise lawful within their home jurisdictions — is the fact that both executive orders define prohibited activities in broad and ambiguous terms, seemingly on a strict liability basis.

Both the GHRAVITY E.O. and the FSE E.O. became effective upon issuance, although it is anticipated that OFAC will follow up with implementing regulations for each executive order in due course. In the meantime, while the consequences of designation are spelled out in both executive orders, the full range of activities, as well as the standard of knowledge, if any, that could trigger sanctions, is currently unclear.

Given the paucity of official interpretive guidance thus far, non-U.S. companies — and the U.S. persons who deal with them — will need to exercise greater vigilance and prudence than ever to ensure that their international business and other dealings comply with the expanding and increasingly extraterritorial universe of U.S. trade controls.

**Key Takeaways (For Now)**

Although their full impact remains to be seen, these new sanctions prompt the following immediate observations:

1) Non-U.S. companies, especially in the telecommunications and information technology sectors, will need to consider carefully whether their products or services are being used by Iran or Syria, even indirectly, in activities that are likely to facilitate cyber-suppression.

- The GHRAVITY E.O. expressly uses the terms “indirectly” and “likely” without defining them, which could lead to unintended exposure for companies that provide seemingly benign technology or services directly to Iran or Syria, or to third parties that deal with those countries, that are not obviously intended to be used for Internet censorship, denial of access to the Internet and other electronic communications media, or electronic surveillance, but which can be applied for such purposes.
  - For example, deep packet inspection technology allows legitimate computer network security management, statistical analysis and identification of cyber-threats such as viruses, spam, and unauthorized intrusion. But it can also be used for data mining, eavesdropping and censorship.
• In addition, the full range of activities that would constitute such cyber-suppression is also undefined.
  o For example, where is the line drawn between arguably legitimate activities that further enhance network security or national security and those that “assist” or “enable” human rights abuses?
  o It is entirely conceivable that OFAC could interpret information technology security practices commonly employed in the United States and elsewhere as associated with human rights abuses when used in the same or similar manner by Iran or Syria.

• How many degrees removed from the ultimate end use by Iran or Syria are necessary to foreclose liability?
  o Will there be any safe harbors available through contractual limitations against using technology or services for purposes set forth in the GHRAVITY E.O.?
  o Will strict liability be enforced or will some degree of knowledge be required? This is important, since the consequences of being designated under the order (i.e., blocking) are the same employed against terrorists, narcotraffickers, and embargoed countries themselves.

2) The FSE E.O. extends OFAC’s power to deter non-U.S. “sanctions-busters” by exposing them to consequences for inducing U.S. persons to violate sanctions and/or obscuring an ultimate beneficial interest of Iran or Syria in a transaction.

• It also exposes to potential liability non-U.S. companies that distribute or resell downstream U.S.-origin items or items with certain levels of U.S.-origin content, even unwittingly.

• Although non-U.S. companies are obliged to follow existing limitations on re-exporting certain U.S.-origin items to Iran or Syria, now the consequences for even unintentionally doing so potentially include a full-scale denial of access to U.S. commerce.

• The prohibition against facilitating deceptive transactions could affect all non-U.S. parties that become involved in a transaction in which Iran or Syria has an ultimate beneficial interest and that involves some connection to the United States, even if the activities occur wholly offshore and the parties are unaware of the sanctions issue.
  o For example, transportation providers, freight forwarders, financial institutions, insurers and other parties involved in a transaction could be deemed to be unlawful facilitators if some aspect of the transaction is tainted under the relevant sanctions, even if they themselves are unaware that another party to the transaction engaged in a deceptive activity, such as “white labeling” goods to obscure their source.
3) Overall, both new executive orders create an uncertain environment, in which the U.S. government is empowered to deny non-U.S. companies that have some business interest with Iran or Syria — however remote — access to U.S. commerce.

- Non-U.S. companies, therefore, will need to balance the risks of such consequences against their current business profiles.

- Finally, it is unclear whether these new sanctions measures will be applied prospectively only or whether they could reach prior conduct.

--By Mario Mancuso, Jay Kraemer, Robert Mollen, John Pisa-Relli, Tobias Caspary, Melina Kapeliou, Melissa D’Arcy and Maria Cirincione, Fried Frank Harris Shriver & Jacobson LLP

Mario Mancuso is a partner in Fried Frank’s Washington, D.C., office, where he chairs the firm’s international trade and investment practice. Jay Kraemer is of counsel in the firm’s Washington office. Robert Mollen is a partner in the firm’s London office. John Pisa-Relli is special counsel in the firm’s Washington office. Tobias Caspary and Melina Kapeliou are associates in the firm’s London office. Melissa D’Arcy and Maria Cirincione are associates in the firm’s Washington office.

The opinions expressed are those of the authors and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] While neither executive order explicitly states so, it is presumed that U.S. persons that engage in unauthorized dealings with the targets of these new sanctions will be subject to the standard civil and criminal penalties prescribed under the International Emergency Economic Powers Act, which is the principal statutory authority for both executive orders; e.g., civil penalties of up to the greater of $250,000 per incident or twice the transaction value, criminal penalties of up to $1 million and up to 20 years imprisonment for individual criminal misconduct, and other consequences, such as blocked funds under the GHRAVITY E.O., and seized goods, export denial and other potential consequences under both executive orders.

All Content © 2003-2012, Portfolio Media, Inc.