DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

A Framework for OFAC Compliance Commitments

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) administers and enforces U.S. economic and trade sanctions programs against targeted foreign governments, individuals, groups, and entities in accordance with national security and foreign policy goals and objectives.

OFAC strongly encourages organizations subject to U.S. jurisdiction, as well as foreign entities that conduct business in or with the United States, U.S. persons, or using U.S.-origin goods or services, to employ a risk-based approach to sanctions compliance by developing, implementing, and routinely updating a sanctions compliance program (SCP). While each risk-based SCP will vary depending on a variety of factors—including the company's size and sophistication, products and services, customers and counterparties, and geographic locations—each program should be predicated on and incorporate at least five essential components of compliance: (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training.

If after conducting an investigation and determining that a civil monetary penalty ("CMP") is the appropriate administrative action in response to an apparent violation, the Office of Compliance and Enforcement (OCE) will determine which of the following or other elements should be incorporated into the subject person's SCP as part of any accompanying settlement agreement, as appropriate. As in all enforcement cases, OFAC will evaluate a subject person's SCP in a manner consistent with the Economic Sanctions Enforcement Guidelines (the "Guidelines").

When applying the Guidelines to a given factual situation, OFAC will consider favorably subject persons that had effective SCPs at the time of an apparent violation. For example, under General Factor E (compliance program), OFAC may consider the existence, nature, and adequacy of an SCP, and when appropriate, may mitigate a CMP on that basis. Subject persons that have implemented effective SCPs that are predicated on the five essential components of compliance may also benefit from further mitigation of a CMP pursuant to General Factor F (remedial response) when the SCP results in remedial steps being taken.

Finally, OFAC may, in appropriate cases, consider the existence of an effective SCP at the time of an apparent violation as a factor in its analysis as to whether a case is deemed "egregious."

This document is intended to provide organizations with a framework for the five essential components of a risk-based SCP, and contains an appendix outlining several of the root causes that have led to apparent violations of the sanctions programs that OFAC administers. OFAC recommends all organizations subject to U.S. jurisdiction review the settlements published by OFAC to reassess and enhance their respective SCPs, when and as appropriate.

MANAGEMENT COMMITMENT

Senior Management's commitment to, and support of, an organization's risk-based SCP is one of the most important factors in determining its success. This support is essential in ensuring the SCP receives adequate resources and is fully integrated into the organization's daily operations, and also helps legitimize the program, empower its personnel, and foster a culture of compliance throughout the organization.

General Aspects of an SCP: Senior Management Commitment

Senior management commitment to supporting an organization's SCP is a critical factor in determining the success of the SCP. Effective management support includes the provision of adequate resources to the compliance unit(s) and support for compliance personnel's authority within an organization. The term "senior management" may differ among various organizations, but typically the term should include senior leadership, executives, and/or the board of directors.

I. Senior management has reviewed and approved the organization's SCP.

II. Senior management ensures that its compliance unit(s) is/are delegated sufficient authority and autonomy to deploy its policies and procedures in a manner that effectively controls the organization's OFAC risk. As part of this effort, senior management ensures the existence of direct reporting lines between the SCP function and senior management, including routine and periodic meetings between these two elements of the organization.

III. Senior management has taken, and will continue to take, steps to ensure that the organization's compliance unit(s) receive adequate resources—including in the form of human capital, expertise, information technology, and other resources, as appropriate—that are relative to the organization's breadth of operations, target and secondary markets, and other factors affecting its overall risk profile.

These efforts could generally be measured by the following criteria:

A. The organization has appointed a dedicated OFAC sanctions compliance officer[1];
B. The quality and experience of the personnel dedicated to the SCP, including: (i) the technical knowledge and expertise of these personnel with respect to OFAC's regulations, processes, and actions; (ii) the ability of these personnel to understand complex financial and commercial activities, apply their knowledge of OFAC to these items, and identify OFAC-related issues, risks, and prohibited activities; and (iii) the efforts to ensure that personnel dedicated to the SCP have sufficient experience and an appropriate position within the organization, and are an integral component to the organization's success; and

[1] This may be the same person serving in other senior compliance positions, e.g., the Bank Secrecy Act Officer or an Export Control Officer, as many institutions, depending on size and complexity, designate a single person to oversee all areas of financial crimes or export control compliance.

C. Sufficient control functions exist that support the organization's SCP—including but not limited to information technology software and systems—that adequately address the organization's OFAC-risk assessment and levels.

IV. Senior management promotes a "culture of compliance" throughout the organization.

These efforts could generally be measured by the following criteria:

A. The ability of personnel to report sanctions related misconduct by the organization or its personnel to senior management without fear of reprisal.
B. Senior management messages and takes actions that discourage misconduct and prohibited activities, and highlight the potential repercussions of non-compliance with OFAC sanctions; and
C. The ability of the SCP to have oversight over the actions of the entire organization, including but not limited to senior management, for the purposes of compliance with OFAC sanctions.

V. Senior management demonstrates recognition of the seriousness of apparent violations of the laws and regulations administered by OFAC, or malfunctions, deficiencies, or failures by the organization and its personnel to comply with the SCP's policies and procedures, and implements necessary measures to reduce the occurrence of apparent violations in the future. Such measures should address the root causes of past apparent violations and represent systemic solutions whenever possible.

RISK ASSESSMENT

Risks in sanctions compliance are potential threats or vulnerabilities that, if ignored or not properly handled, can lead to violations of OFAC's regulations and negatively affect an organization's reputation and business. OFAC recommends that organizations take a risk-based approach when designing or updating an SCP. One of the central tenets of this approach is for organizations to conduct a routine, and if appropriate, ongoing "risk assessment" for the purposes of identifying potential OFAC issues they are likely to encounter. As described in detail below, the results of a risk assessment are integral in informing the SCP's policies, procedures, internal controls, and training in order to mitigate such risks.

While there is no "one-size-fits all" risk assessment, the exercise should generally consist of a holistic review of the organization from top-to-bottom and assess its touchpoints to the outside world. This process allows the organization to identify potential areas in which it may, directly or indirectly, engage with OFAC-prohibited persons, parties, countries, or regions. For example, an organization's SCP may conduct an assessment of the following: (i) customers, supply chain, intermediaries, and counter-parties; (ii) the products and services it offers, including how and where such items fit into other financial or commercial products, services, networks, or systems; and (iii) the geographic locations of the organization, as well as its customers, supply chain, intermediaries, and counter-parties. Risk assessments and sanctions-related due diligence is also

important during mergers and acquisitions, particularly in scenarios involving non-U.S. companies or corporations.

General Aspects of an SCP: Conducting a Sanctions Risk Assessment

A fundamental element of a sound SCP is the assessment of specific clients, products, services, and geographic locations in order to determine potential OFAC sanctions risk. The purpose of a risk assessment is to identify inherent risks in order to inform risk-based decisions and controls. The Annex to Appendix A to 31 C.F.R. Part 501, OFAC's Economic Sanctions Enforcement Guidelines, provides an OFAC Risk Matrix that may be used by financial institutions or other entities to evaluate their compliance programs:

I. The organization conducts, or will conduct, an OFAC risk assessment in a manner, and with a frequency, that adequately accounts for the potential risks. Such risks could be posed by its clients and customers, products, services, supply chain, intermediaries, counter-parties, transactions, and geographic locations, depending on the nature of the organization. As appropriate, the risk assessment will be updated to account for the root causes of any apparent violations or systemic deficiencies identified by the organization during the routine course of business.

A. In assessing its OFAC risk, organizations should leverage existing information to inform the process. In turn, the risk assessment will generally inform the extent of the due diligence efforts at various points in a relationship or in a transaction. This may include:

1. On-boarding: The organization develops a sanctions risk rating for customers, customer groups, or account relationships, as appropriate, by leveraging information provided by the customer (for example, through a Know Your Customer or Customer Due Diligence process) and independent research conducted by the organization at the initiation of the customer relationship. This information will guide the timing and scope of future due diligence efforts. Important elements to consider in determining the sanctions risk rating can be found in OFAC's risk matrices.
2. Mergers and Acquisitions (M&A): As noted above, proper risk assessments should include and encompass a variety of factors and data points for each organization. One of the multitude of areas organizations should include in their risk assessments—which, in recent years, appears to have presented numerous challenges with respect to OFAC sanctions—are mergers and acquisitions. Compliance functions should also be integrated into the merger, acquisition, and integration process. Whether in an advisory capacity or as a participant, the organization engages in appropriate due diligence to ensure that sanctions-related issues are identified, escalated to the relevant senior levels, addressed prior to the conclusion of any transaction, and incorporated into the organization's risk assessment process. After an M&A transaction is

completed, the organization's Audit and Testing function will be critical to identifying any additional sanctions-related issues.

II. The organization has developed a methodology to identify, analyze, and address the particular risks it identifies. As appropriate, the risk assessment will be updated to account for the conduct and root causes of any apparent violations or systemic deficiencies identified by the organization during the routine course of business, for example, through a testing or audit function.

INTERNAL CONTROLS

An effective SCP should include internal controls, including policies and procedures, in order to identify, interdict, escalate, report (as appropriate), and keep records pertaining to activity that may be prohibited by the regulations and laws administered by OFAC. The purpose of internal controls is to outline clear expectations, define procedures and processes pertaining to OFAC compliance (including reporting and escalation chains), and minimize the risks identified by the organization's risk assessments. Policies and procedures should be enforced, weaknesses should be identified (including through root cause analysis of any compliance breaches) and remediated, and internal and/or external audits and assessments of the program should be conducted on a periodic basis.

Given the dynamic nature of U.S. economic and trade sanctions, a successful and effective SCP should be capable of adjusting rapidly to changes published by OFAC. These include the following: (i) updates to OFAC's List of Specially Designated Nationals and Blocked Persons (the "SDN List"), the Sectoral Sanctions Identification List ("SSI List"), and other sanctions-related lists; (ii) new, amended, or updated sanctions programs or prohibitions imposed on targeted foreign countries, governments, regions, or persons, through the enactment of new legislation, the issuance of new Executive orders, regulations, or published OFAC guidance or other OFAC actions; and (iii) the issuance of general licenses.

General Aspects of an SCP: Internal Controls

Effective OFAC compliance programs generally include internal controls, including policies and procedures, in order to identify, interdict, escalate, report (as appropriate), and keep records pertaining to activity that is prohibited by the sanctions programs administered by OFAC. The purpose of internal controls is to outline clear expectations, define procedures and processes pertaining to OFAC compliance, and minimize the risks identified by an entity's OFAC risk assessments. Policies and procedures should be enforced, and weaknesses should be identified (including through root cause analysis of any compliance breaches) and remediated in order to prevent activity that might violate the sanctions programs administered by OFAC.

I. The organization has designed and implemented written policies and procedures outlining the SCP. These policies and procedures are relevant to the organization, capture the organization's day-to-day operations and procedures, are easy to follow, and designed to prevent employees from engaging in misconduct.

II. The organization has implemented internal controls that adequately address the results of its OFAC risk assessment and profile. These internal controls should enable the organization to clearly and effectively identify, interdict, escalate, and report to appropriate personnel within the organization transactions and activity that may be prohibited by OFAC. To the extent information technology solutions factor into the organization's internal controls, the organization has selected and calibrated the solutions in a manner that is appropriate to address the organization's risk profile and compliance needs, and the organization routinely tests the solutions to ensure effectiveness.

III. The organization enforces the policies and procedures it implements as part of its OFAC compliance internal controls through internal and/or external audits.

IV. The organization ensures that its OFAC-related recordkeeping policies and procedures adequately account for its requirements pursuant to the sanctions programs administered by OFAC.

V. The organization ensures that, upon learning of a weakness in its internal controls pertaining to OFAC compliance, it will take immediate and effective action, to the extent possible, to identify and implement compensating controls until the root cause of the weakness can be determined and remediated.

VI. The organization has clearly communicated the SCP's policies and procedures to all relevant staff, including personnel within the SCP program, as well as relevant gatekeepers and business units operating in high-risk areas (e.g., customer acquisition, payments, sales, etc.) and to external parties performing SCP responsibilities on behalf of the organization.

VII. The organization has appointed personnel for integrating the SCP's policies and procedures into the daily operations of the company or corporation. This process includes consultations with relevant business units, and confirms the organization's employees understand the policies and procedures.

TESTING AND AUDITING

Audits assess the effectiveness of current processes and check for inconsistencies between these and day-to-day operations. A comprehensive and objective testing or audit function within an SCP ensures that an organization identifies program weaknesses and deficiencies, and it is the organization's responsibility to enhance its program, including all program-related software, systems, and other technology, to remediate any identified compliance gaps. Such enhancements might include updating, improving, or recalibrating SCP elements to account for a changing risk assessment or sanctions environment. Testing and auditing can be conducted on a specific element of an SCP or at the enterprise-wide level.

General Aspects of an SCP: Testing and Auditing

A comprehensive, independent, and objective testing or audit function within an SCP ensures that entities are aware of where and how their programs are performing and should be updated, enhanced, or recalibrated to account for a changing risk assessment or sanctions environment, as appropriate. Testing or audit, whether conducted on a specific element of a compliance program or at the enterprise-wide level, are important tools to ensure the program is working as designed and identify weaknesses and deficiencies within a compliance program.

I. The organization commits to ensuring that the testing or audit function is accountable to senior management, is independent of the audited activities and functions, and has sufficient authority, skills, expertise, resources, and authority within the organization.

II. The organization commits to ensuring that it employs testing or audit procedures appropriate to the level and sophistication of its SCP and that this function, whether deployed internally or by an external party, reflects a comprehensive and objective assessment of the organization's OFAC-related risk assessment and internal controls.

III. The organization ensures that, upon learning of a confirmed negative testing result or audit finding pertaining to its SCP, it will take immediate and effective action, to the extent possible, to identify and implement compensating controls until the root cause of the weakness can be determined and remediated.

TRAINING

An effective training program is an integral component of a successful SCP. The training program should be provided to all appropriate employees and personnel on a periodic basis (and at a minimum, annually) and generally should accomplish the following: (i) provide job-specific knowledge based on need; (ii) communicate the sanctions compliance responsibilities for each employee; and (iii) hold employees accountable for sanctions compliance training through assessments.

General Aspects of an SCP: Training

An adequate training program, tailored to an entity's risk profile and all appropriate employees and stakeholders, is critical to the success of an SCP.

I. The organization commits to ensuring that its OFAC-related training program provides adequate information and instruction to employees and, as appropriate, stakeholders (for example, clients, suppliers, business partners, and counterparties) in order to support the organization's OFAC compliance efforts. Such training should be further tailored to high-risk employees within the organization.

II. The organization commits to provide OFAC-related training with a scope that is appropriate for the products and services it offers; the customers, clients, and partner relationships it maintains; and the geographic regions in which it operates.

III. The organization commits to providing OFAC-related training with a frequency that is appropriate based on its OFAC risk assessment and risk profile.

IV. The organization commits to ensuring that, upon learning of a confirmed negative testing result or audit finding, or other deficiency pertaining to its SCP, it will take immediate and effective action to provide training to or other corrective action with respect to relevant personnel.

V. The organization's training program includes easily accessible resources and materials that are available to all applicable personnel.

Root Causes of OFAC Sanctions Compliance Program Breakdowns or Deficiencies Based on Assessment of Prior OFAC Administrative Actions

Since its publication of the Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, App. A (the "Guidelines"), OFAC has finalized numerous public enforcement actions in which it identified deficiencies or weaknesses within the subject person's SCP. These items, which are provided in a non-exhaustive list below, are provided to alert persons subject to U.S. jurisdiction, including entities that conduct business in or with the United States, U.S. persons, or U.S.-origin goods or services, about several specific root causes associated with apparent violations of the regulations it administers in order to assist them in designing, updating, and amending their respective SCP.

I. Lack of a Formal OFAC SCP

OFAC regulations do not require a formal SCP; however, OFAC encourages organizations subject to U.S. jurisdiction (including but not limited to those entities that conduct business in, with, or through the United States or involving U.S.-origin goods, services, or technology), and particularly those that engage in international trade or transactions or possess any clients or counter-parties located outside of the United States, to adopt a formal SCP. OFAC has finalized numerous civil monetary penalties since publicizing the Guidelines in which the subject person's lack of an SCP was one of the root causes of the sanctions violations identified during the course of the investigation. In addition, OFAC frequently identified this element as an aggravating factor in its analysis of the General Factors associated with such administrative actions.

II. Misinterpreting, or Failing to Understand the Applicability of, OFAC's Regulations

Numerous organizations have committed sanctions violations by misinterpreting OFAC's regulations, particularly in instances in which the subject person determined the transaction, dealing, or activity at issue was either not prohibited or did not apply to their organization or operations. For example, several organizations have failed to appreciate or consider (or, in some instances, actively disregarded) the fact that OFAC sanctions applied to their organization based on their status as a U.S. person, a U.S.-owned or controlled subsidiary (in the Cuba and Iran programs), or dealings in or with U.S. persons, the U.S. financial system, or U.S.-origin goods and technology.

With respect to this specific root cause, OFAC's administrative actions have typically identified additional aggravating factors, such as reckless conduct, the presence of numerous warning signs that the activity at issue was likely prohibited, awareness by the organization's management of the conduct at issue, and the size and sophistication of the subject person.

III. Facilitating Transactions by Non-U.S. Persons (Including Through or By Overseas Subsidiaries or Affiliates)

Multiple organizations subject to U.S. jurisdiction—specifically those with foreign-based operations and subsidiaries located outside of the United States—have engaged in transactions or activity that violated OFAC's regulations by referring business opportunities to, approving or

signing off on transactions conducted by, or otherwise facilitating dealings between their organization's non-U.S. locations and OFAC-sanctioned countries, regions, or persons. In many instances, the root cause of these violations stems from a misinterpretation or misunderstanding of OFAC's regulations. Companies and corporations with integrated operations, particularly those involving or requiring participation by their U.S.-based headquarters, locations, or personnel, should ensure any activities they engage in (i.e., approvals, contracts, procurement, etc.) are compliant with OFAC's regulations.

IV. Exporting or Re-exporting U.S.-origin Goods, Technology, or Services to OFAC-Sanctioned Persons or Countries

Non-U.S. persons have repeatedly purchased U.S.-origin goods with the specific intent of re-exporting, transferring, or selling the items to a person, country, or region subject to OFAC sanctions. In several instances, this activity occurred despite warning signs that U.S. economic sanctions laws prohibited the activity, including contractual language expressly prohibiting any such dealings. OFAC's public enforcement actions in this area have generally been focused on companies or corporations that are large or sophisticated, engaged in a pattern or practice that lasted multiple years, ignored or failed to respond to numerous warning signs, utilized non-routine business practices, and—in several instances—concealed their activity in a willful or reckless manner.

V. Utilizing the U.S. Financial System, or Processing Payments to or through U.S. Financial Institutions, for Commercial Transactions Involving OFAC-Sanctioned Persons or Countries

Many non-U.S. persons have engaged in violations of OFAC's regulations by processing financial transactions (almost all of which have been denominated in U.S. Dollars) to or through U.S. financial institutions that pertain to commercial activity involving an OFAC-sanctioned country, region, or person. Although no organizations subject to U.S. jurisdiction may be involved in the underlying transaction—such as the shipment of goods from a third-country to an OFAC-sanctioned country—the inclusion of a U.S. financial institution in any payments associated with these transactions often results in a prohibited activity (e.g., the exportation or re-exportation of services from the United States to a comprehensively sanctioned country, or dealing in blocked property in the United States). OFAC has generally focused its enforcement investigations on persons who have engaged in willful or reckless conduct, attempted to conceal their activity (e.g., by stripping or manipulating payment messages, or making false representations to their non-U.S. or U.S. financial institution), engaged in a pattern or practice of conduct for several months or years, ignored or failed to consider numerous warning signs that the conduct was prohibited, involved actual knowledge or involvement by the organization's management, caused significant harm to U.S. sanctions program objectives, and were large or sophisticated organizations.

VI. Sanctions Screening Software or Filter Faults

Many organizations conduct screening of their customers, supply chain, intermediaries, counter-parties, commercial and financial documents, and transactions in order to identify OFAC-prohibited locations, parties, or dealings. At times, organizations have failed to update their sanctions screening software to incorporate updates to the SDN List or SSI List, failed to include pertinent identifiers such as SWIFT Business Identifier Codes for designated, blocked, or sanctioned financial institutions, or did not account for alternative spellings of prohibited countries or parties—particularly in instances in which the organization is domiciled or conducts business in geographies that frequently utilize such alternative spellings (i.e., Habana instead of Havana, Kuba instead of Cuba, Soudan instead of Sudan, etc.),

VII. Improper Due Diligence on Customers/Clients (e.g., Ownership, Business Dealings, etc.)

One of the fundamental components of an effective OFAC risk assessment and SCP is conducting due diligence on an organization's customers, supply chain, intermediaries, and counter-parties. Various administrative actions taken by OFAC involved improper or incomplete due diligence by a company or corporation on its customers, such as their ownership, geographic location(s), counter-parties, and transactions, as well as their knowledge and awareness of OFAC sanctions.

VIII. De-Centralized Compliance Functions and Inconsistent Application of an SCP

While each organization should design, develop, and implement its risk-based SCP based on its own characteristics, several organizations subject to U.S. jurisdiction have committed apparent violations due to a de-centralized SCP, often with personnel and decision-makers scattered in various offices or business units. In particular, violations have resulted from this arrangement due to an improper interpretation and application of OFAC's regulations, the lack of a formal escalation process to review high-risk or potential OFAC customers or transactions, an inefficient or incapable oversight and audit function, or miscommunications regarding the organization's sanctions-related policies and procedures.

IX. Utilizing Non-Standard Payment or Commercial Practices

Organizations subject to U.S. jurisdiction are in the best position to determine whether a particular dealing, transaction, or activity is proposed or processed in a manner that is consistent with industry norms and practices. In many instances, organizations attempting to evade or circumvent OFAC sanctions or conceal their activity will implement non-traditional business methods in order to complete their transactions.

X. Individual Liability

In several instances, individual employees—particularly in supervisory, managerial, or executive-level positions—have played integral roles in causing or facilitating violations of the regulations administered by OFAC. Specifically, OFAC has identified scenarios involving U.S.-owned or controlled entities operating outside of the United States, in which supervisory, managerial or executive employees of the entities conducted or facilitated dealings or transactions with OFAC-sanctioned persons, regions, or countries, notwithstanding the fact that the U.S. entity had a fulsome sanctions compliance program in place. In some of these cases, the employees of the foreign entities also made efforts to obfuscate and conceal their activities from others within the corporate organization, including compliance personnel, as well as from regulators or law enforcement. In such circumstances, OFAC will consider using its enforcement authorities not only against the violating entities, but against the individuals as well.