How OFAC Sanctions Work

A Practitioner's Reference Guide to the U.S. Sanctions Framework

Authorities • Prohibitions • Lists • Licensing • Enforcement • Compliance

A foundational, program-neutral guide to the machinery common to every OFAC sanctions program — the statutory architecture, the difference between blocking and prohibition, the sanctions lists and the 50% Rule, general and specific licensing, and how OFAC enforces.

Published by mrsanctions.com

Burnin', Briefly: Hot Takes from Mr. Sanctions

Contents

1. How to Use This Guide

HOW TO USE THIS GUIDE

This guide explains the framework that is common to **every** OFAC sanctions program. It is not a substitute for the program-specific guides (Iran, Russia, Cuba, Venezuela, and so on); it is the layer beneath them. Use it as follows:

- **Building or auditing a compliance program:** Sections 7 (Compliance Program Framework) and 8 (Transaction-Level Checklist).
- **Screening a counterparty:** Sections 4 (Lists) and 5 (the 50% Rule), then the relevant program guide.
- **Determining whether a transaction is prohibited:** Section 3 (Prohibition Types) and Section 6 (Licensing and Exemptions).
- **Understanding penalties and self-disclosure:** Section 9 (Enforcement).
- **Orienting to the legal hierarchy:** Section 2 (Authorities and Framework).

CRITICAL — DO NOT REASON BY ANALOGY ACROSS PROGRAMS

The single most common mistake practitioners make is assuming that a rule learned in one program carries over to another. It frequently does not. The 50% Rule, general licenses, exemptions, the definition of who is a "U.S. person," and even the meaning of "blocking" versus "restriction" vary by program and by the legal instrument involved. A general license under one Executive order does **not** authorize anything under a different program. Comprehensive embargoes (e.g., Cuba, Iran) block entire categories of persons by status, not just listed names. Always confirm the rule in the specific program's regulations before acting.

2. The Legal Architecture: Authorities and Framework

OFAC does not write sanctions policy on a blank slate. Every program sits in a hierarchy that runs from a statute, through a presidential Executive order, into OFAC's codified regulations, and finally into the operational instruments (directives, general licenses, and designations) that practitioners deal with day to day. Understanding the hierarchy tells you where to look when the regulations are silent and how durable a given rule is.

2.1 The statutory layer

Most modern OFAC programs rest on the International Emergency Economic Powers Act (IEEPA), codified at 50 U.S.C. §§ 1701–1706. IEEPA lets the President, after declaring a national emergency with respect to an "unusual and extraordinary threat" that has its source in whole or substantial part outside the United States, regulate or prohibit a broad range of transactions and block property in which a foreign interest exists. IEEPA is the engine behind the Russia, Iran (in part), Venezuela, counter-terrorism, counter-narcotics, and most thematic programs.

A national emergency under IEEPA must be declared and annually renewed under the National Emergencies Act (NEA), 50 U.S.C. §§ 1601–1651. When the underlying emergency lapses or is terminated, the IEEPA-based prohibitions tied to it fall away. A handful of programs — most notably Cuba — rest instead on the older Trading with the Enemy Act (TWEA), 50 U.S.C. §§ 4301–4341, which predates IEEPA and is continued annually by presidential determination. Other programs draw on freestanding statutes (for example, the Foreign Narcotics Kingpin Designation Act, CAATSA, and various country-specific acts) that supply their own designation criteria and, often, secondary-sanctions authority.

2.2 The Executive order layer

Within the authority a statute grants, the President issues Executive orders (E.O.s) that declare the emergency, name the threat, set out the blocking and prohibition criteria, and delegate implementation to the Secretary of the Treasury (and thus to OFAC). The E.O. is where you find the operative designation criteria — the conduct or status that makes a person a target. Amendments and new E.O.s expand or narrow programs over time; the program-specific guide is the place to track a given program's E.O. lineage.

2.3 The regulatory layer (31 CFR Chapter V)

OFAC codifies each program in its own part of 31 CFR Chapter V (for example, the Cuban Assets Control Regulations at Part 515, the Iranian Transactions and Sanctions Regulations at Part 560). Cutting across all of them is 31 CFR Part 501, the Reporting, Procedures and Penalties Regulations. Part 501 is program-neutral: it sets the recordkeeping requirements (§ 501.601), the reports OFAC can demand (§ 501.602), the licensing procedures (§ 501.801), and — in its Appendix A — the Economic Sanctions Enforcement Guidelines. Substantive prohibitions live in each program's own part; the cross-cutting mechanics live in Part 501.

2.4 The operational layer

Below the regulations are the instruments practitioners touch most: **directives** (which impose specific prohibitions on named sectors or persons, common in the Russia program), **designations** (additions to the SDN or other lists), **general licenses** (self-executing authorizations), and **FAQs and guidance** (interpretive, non-binding but authoritative in practice). OFAC catalogs current statutes, E.O.s, regulations, and guidance for each program on its Sanctions Programs and Country Information page.

> **KEY COMPLIANCE TAKEAWAY**
> When a question is not answered by a program's own regulations, the answer usually lives one layer up (the E.O. or statute) or in the cross-cutting Part 501 — not by analogy to another program.

3. What OFAC Sanctions Actually Prohibit

OFAC programs do not all do the same thing. The prohibitions fall into a small number of recurring types. Identifying which type applies is the first analytical step in any transaction review.

3.1 Blocking (asset freezes)

Blocking is the core sanctions tool. When a person's property and interests in property are blocked, all property and interests in property that are in the United States or in the possession or control of a U.S. person are frozen: they cannot be transferred, paid, withdrawn, exported, or otherwise dealt in. Blocking is immediate and across-the-board — it is not a seizure (title does not pass to the government), but the U.S. person holding the property must place it into a blocked account and report it. A "U.S. person" generally means U.S. citizens and permanent residents wherever located, entities organized under U.S. law (including foreign branches), and anyone physically in the United States.

> **CRITICAL DISTINCTION — BLOCK vs. REJECT**
> Blocking and rejecting are different obligations, and choosing the wrong one is itself a violation. If a transaction involves a blocked person's property interest, the U.S. person must **block** it (freeze and hold the funds, then report). If a transaction is merely prohibited — for example, an unlicensed dealing with a comprehensively embargoed jurisdiction that does not involve a blocked party's property — the U.S. person typically must **reject** it (refuse to process and return it). Returning blocked funds, or holding rejected funds, both create liability. *(FAQ #127)*

3.2 Comprehensive (embargo) programs

A handful of programs are comprehensive: they prohibit virtually all transactions with an entire jurisdiction, its government, and (in some cases) its nationals, regardless of whether any specific party appears on a list. Cuba, Iran, North Korea, Syria (historically), and the Crimea/so-called DNR/LNR regions of Ukraine are the principal examples. In a comprehensive program, the absence of a counterparty from the SDN List is meaningless — the jurisdiction itself is the target, and entire classes of persons are blocked or restricted by status. This is the clearest example of why list-screening alone is never sufficient.

3.3 Selective / list-based programs

Most programs are selective: they target specific designated persons (and those owned 50% or more by them — see Section 5) rather than a whole country. Russia, Venezuela, counter-terrorism, counter-narcotics, cyber, and the Global Magnitsky human-rights program work this way. Here the SDN List and the 50% Rule do most of the work, supplemented by sectoral restrictions in some programs.

3.4 Sectoral and menu-based restrictions

Some programs stop short of full blocking. Sectoral sanctions (the Russia Sectoral Sanctions Identifications, or SSI, List is the classic example) prohibit only certain dealings — new debt of a specified maturity, new equity, or particular services — with named persons whose other property is not frozen. "Menu-based" statutory sanctions (e.g., under CAATSA) let the President select from a list of possible measures to impose on a person who engages in covered conduct. These are easy to mishandle because the counterparty is not blocked: ordinary transactions remain permissible while the specifically restricted ones are not.

> **NOTE — NO 50% RULE HALO ON SOME NON-BLOCKING LISTS**
>
> The 50% Rule (Section 5) attaches to **blocked** persons. Whether it extends to a non-blocking list depends on the list. It applies to SSI List entries for purposes of the sectoral prohibitions, but the analysis differs from SDN blocking. Do not assume uniform treatment — check the program.

3.5 Secondary sanctions

Primary sanctions bind U.S. persons. Secondary sanctions instead threaten *non-U.S. persons* with loss of access to the U.S. market or financial system if they engage in specified activity with sanctioned targets — even where no U.S. nexus exists. They are a foreign-policy lever, not a direct prohibition, and they typically lack the safe harbors and general licenses that primary prohibitions carry. Secondary-sanctions exposure is the reason non-U.S. financial institutions screen against OFAC lists at all.

> **CRITICAL — SECONDARY SANCTIONS HAVE NO SAFE HARBOR AND NO BRIGHT LINE**
>
> A non-U.S. person generally does not risk being sanctioned for activity that a U.S. person could engage in without a license *(FAQ #7)*. But where secondary sanctions apply, there is usually no de minimis threshold and no general license to rely on; the standard is often "significant transaction," judged on a multi-factor, case-by-case basis with no published dollar floor. Treating a small transaction as automatically safe is a recurring and costly error.

> **KEY COMPLIANCE TAKEAWAY**
>
> Before reviewing any transaction, classify the program: comprehensive vs. selective, blocking vs. non-blocking restriction, and primary vs. secondary — because the screening obligation, the licensing options, and the safe harbors all turn on that classification.

4. The Sanctions Lists

OFAC publishes several lists. They are not interchangeable, and the legal consequence of a match depends on which list the name appears on. OFAC distributes the data through its Sanctions List Service and provides a free Sanctions List Search tool that searches the SDN and Consolidated lists together *(FAQ #369)*. Details on the non-SDN lists are on the Additional Sanctions Lists page *(FAQ #422)*.

List	What it means	Legal effect	50% Rule applies?
SDN List (Specially Designated Nationals and Blocked Persons)	Persons whose property is blocked under one or more programs.	Full blocking. Freeze and report all property and interests in property.	**Yes** — entities owned 50%+ in aggregate are blocked even if not listed.
Consolidated (Non-SDN) List	A single data file aggregating the non-blocking lists (SSI, NS-MBS, and others).	Varies by component list; generally not full blocking.	Depends on component list.
SSI List (Sectoral Sanctions Identifications)	Russia-program persons subject to sectoral debt/equity/services limits.	Restriction on specified dealings only; other property not frozen.	Yes, for the sectoral prohibitions.
NS-MBS / other Non-SDN lists	Persons subject to specific, non-blocking measures (e.g., correspondent-account limits).	Program-specific restriction, not blocking.	Generally no — confirm per program.
Status-based blocking (no listing)	Cuban nationals, blocked governments, and 50%-owned entities — blocked without appearing by name.	Full blocking by status/operation of law.	N/A — blocking arises by status, not a list entry.

CRITICAL — A "NO HITS" SCREEN IS NOT A CLEAN RESULT

Many persons are blocked without ever appearing on a list: most Cuban nationals, blocked foreign governments, and any entity owned 50% or more by blocked persons under the 50% Rule. A counterparty that returns no list match can still be wholly blocked. List-screening is necessary but never sufficient — jurisdiction, ownership, and status analysis must run alongside it.

KEY COMPLIANCE TAKEAWAY

Identify which list a match is on before deciding what to do: an SDN hit means block, an SSI/Non-SDN hit means apply only the specific restriction, and a clean screen does not rule out status-based or ownership-based blocking.

5. The 50% Rule

OFAC's 50% Rule is the most important unwritten-on-the-list concept in U.S. sanctions. Under OFAC's Revised Guidance of August 13, 2014, any entity owned 50 percent or more, in the aggregate, directly or indirectly, by one or more blocked persons is **itself blocked** — automatically, by operation of the rule, whether or not it appears on the SDN List.

5.1 Aggregation across blocked persons and across programs

Ownership is aggregated. If Blocked Person X owns 25% of an entity and Blocked Person Y owns another 25%, the entity is blocked, because blocked persons own 50% or more in the aggregate *(FAQ #399)*. Critically, the ownership interests of persons blocked under *different* OFAC programs are aggregated together for this purpose — a counter-narcotics SDN's stake and a Russia SDN's stake combine.

5.2 Indirect (layered) ownership

"Indirectly" means ownership through one or more intermediate entities that are themselves 50%-or-more owned by blocked persons. A blocked person who owns 50%+ of Entity A, which owns 50%+ of Entity B, blocks both A and B *(FAQ #401)*. Layered structures must be unwound to their ultimate beneficial owners.

5.3 The 50% Rule speaks to ownership, not control

CRITICAL DISTINCTION — OWNERSHIP, NOT CONTROL (BUT MIND THE GAP)

The 50% Rule is purely an **ownership** test. An entity that is controlled — but not 50%+ owned — by blocked persons is **not** automatically blocked under this rule. But that is not the end of the analysis: OFAC expressly warns against dealing with entities in which blocked persons hold a significant minority stake or exercise control, because OFAC may designate them at any time, and some programs (Cuba, Iran, North Korea, Syria, Venezuela, Crimea) block persons by **control or status** under separate criteria that do not depend on the 50% Rule at all. A 49% blocked stake plus control is a high-risk relationship, not a safe one.

KEY COMPLIANCE TAKEAWAY

Treat any entity that is 50%+ owned in the aggregate by blocked persons as blocked even if it is not on the SDN List; treat significant-minority or controlled entities as high-risk and diligence them as if they could be designated tomorrow.

6. Authorizations: Exemptions, General Licenses, and Specific Licenses

Because the prohibitions are broad, the system relies on three escape valves. Distinguishing them correctly determines whether you may act unilaterally, must apply to OFAC, or may not act at all.

6.1 Exemptions

Exemptions are carve-outs written into the statute itself — most importantly the IEEPA exemptions for personal communications, information and informational materials, and transactions ordinarily incident to travel (the "Berman" exemptions). Because they are statutory, OFAC cannot revoke them by regulation, and they generally apply across IEEPA-based programs. They do **not** apply to TWEA-based programs unless separately provided.

6.2 General licenses

A general license (GL) authorizes a defined category of transactions for everyone who meets its conditions, without any application to OFAC. GLs are self-executing: if your facts fit the GL's terms exactly, you may proceed *(FAQ #7)*. The burden is on you to fit *every* condition; a transaction that misses one element of a GL is simply prohibited. GLs are program-specific — a GL issued under the Russia program authorizes nothing under any other program.

6.3 Specific licenses

A specific license is a written authorization OFAC issues to a particular applicant for a particular transaction, in response to an application filed under the procedures in 31 CFR § 501.801 through OFAC's License Application Page. OFAC reviews each on a case-by-case basis against the program's stated licensing policy *(FAQ #74)*.

KEY LIMIT — NO SPECIFIC LICENSE WHERE A GENERAL LICENSE COVERS YOU

It is OFAC's stated policy not to grant a specific license for a transaction already authorized by an applicable general license. If a GL covers your facts, rely on the GL and document the analysis — do not apply for a specific license *(FAQ #751)*.

NOTE — LICENSE CONDITIONS ARE STRICT AND RECORDS ARE MANDATORY

Persons acting under any license must observe every condition exactly; partial compliance forfeits the authorization. Recordkeeping is not optional — records substantiating reliance on a GL or specific license must be kept for five years under 31 CFR § 501.601, and OFAC can demand them on short notice under § 501.602.

KEY COMPLIANCE TAKEAWAY

Work the authorizations in order — statutory exemption first, then an applicable general license, then a specific license application — and never assume an authorization from one program reaches another.

7. The OFAC Compliance Program Framework

In its Framework for OFAC Compliance Commitments (May 2, 2019), OFAC set out its expectation that every organization with U.S. sanctions exposure maintain a risk-based sanctions compliance program (SCP) built on five essential components. The Framework is not a regulation, and failing to follow it is not itself a violation — but OFAC weighs the existence and quality of an SCP heavily when it decides how to respond to an apparent violation (see Section 9).

Component	What OFAC expects
1. Management commitment	Senior management endorses the program, gives compliance adequate authority and resources, and appoints a dedicated sanctions officer with direct reporting lines.
2. Risk assessment	A documented, recurring assessment of sanctions risk across customers, products, services, supply chains, and geographies — updated for new business, M&A, and program changes.
3. Internal controls	Written policies and procedures, screening and escalation workflows, blocking/rejecting protocols, and recordkeeping that operationalize the risk assessment.
4. Testing and auditing	Independent, periodic testing of the program to find and remediate weaknesses before they become violations.
5. Training	Role-appropriate, recurring training for relevant personnel, with content matched to the organization’s risk profile.

SAFE HARBOR — AN EFFECTIVE SCP IS A MITIGATING FACTOR

Under the Enforcement Guidelines’ General Factor E, OFAC considers a pre-existing, effective compliance program a mitigating factor in any penalty determination, and a strong remedial response (General Factor F) mitigates further. The Framework’s appendix catalogs the recurring "root causes" of violations OFAC sees — absence of a formal SCP, misinterpreting OFAC’s reach, facilitation through non-U.S. affiliates, sanctions screening failures, and decentralized compliance — which doubles as a checklist of what to fix.

KEY COMPLIANCE TAKEAWAY

Build the SCP around the five components and document everything: when a violation occurs, the contemporaneous evidence of a real, risk-based program is what converts a potential enforcement action into a lesser response.

8. Compliance Quick-Reference Checklist

A transaction-level sequence that applies regardless of program. Each step points back to the section that explains it.

1. **Identify every party and jurisdiction.** Originator, beneficiary, intermediaries, vessels, ports, goods origin, and end use. (§ 3)
2. **Classify the relevant program(s).** Comprehensive vs. selective; blocking vs. non-blocking; primary vs. secondary. (§ 3)
3. **Screen against the lists.** SDN and Consolidated lists via the Sanctions List Search tool; record the result. (§ 4)
4. **Run the ownership and status analysis.** Apply the 50% Rule (aggregate, indirect); check for status-based blocking (Cuban nationals, blocked governments). A clean screen is not a clean result. (§§ 4–5)
5. **Determine the obligation if there is a nexus.** Block (freeze + report) or reject (refuse + return) — they are not interchangeable. (§ 3.1)
6. **Look for an authorization.** Statutory exemption → applicable general license → specific license application. Fit every condition. (§ 6)
7. **Report and keep records.** File required blocking/reject reports; retain supporting records for five years per § 501.601. (§§ 6, 9)
8. **Escalate doubt.** Where status, ownership, or licensing is uncertain, hold the transaction and escalate rather than proceed. (§ 1)

9. Enforcement: Liability, Penalties, and Voluntary Disclosure

OFAC enforces under the [Economic Sanctions Enforcement Guidelines] (31 CFR Part 501, Appendix A). Two features drive most outcomes: liability is generally **strict** (intent is not required for civil liability), and the response is calibrated through a set of General Factors.

9.1 Strict liability and the penalty range

A civil violation does not require knowledge or intent — an inadvertent prohibited transaction is still a violation. Civil monetary penalties under IEEPA are inflation-adjusted and substantial (the statutory maximum per violation is recalculated annually), and willful violations can be prosecuted criminally. Because liability is strict, the practical defense is prevention and, failing that, mitigation through the General Factors.

9.2 How OFAC calibrates the response

The Guidelines list eleven General Factors OFAC weighs, including willfulness or recklessness, awareness of the conduct, harm to program objectives, the violator’s sophistication, the quality of the compliance program (Factor E), and the remedial response (Factor F). OFAC’s menu of responses runs from no action, to a cautionary or Finding of Violation letter, to a civil monetary penalty, to referral for criminal prosecution. Two levers most within a company’s control are the SCP it had in place and what it does after discovery.

9.3 Voluntary self-disclosure

A qualifying voluntary self-disclosure (VSD) — notifying OFAC of an apparent violation before OFAC or another agency learns of it through another channel, with a complete report — is a significant mitigating factor that, in a non-egregious case, roughly halves the base penalty under the Guidelines. The combination of a credible SCP and a prompt, complete VSD is the single most effective way to reduce exposure once a problem is found.

9.4 Enforcement read-across

OFAC publishes its civil penalties and enforcement actions so practitioners can calibrate their own programs. The recurring patterns below — drawn from the kinds of root causes OFAC highlights in the Framework appendix and its published enforcement record — show how the abstract rules become liability in practice.

Recurring fact pattern	Mechanism	Compliance implication
Non-U.S. subsidiary processes business with a sanctioned jurisdiction, cleared in USD through a U.S. bank.	U.S. nexus (USD clearing) plus facilitation by the U.S. parent.	Map USD payment flows; a foreign affiliate's transaction can pull the U.S. person in.
Screening engine misses a 50%-owned-but-unlisted entity.	50% Rule blocking with no SDN entry to match against.	Screening must be paired with beneficial-ownership analysis (§ 5).
Firm "rejects" funds that should have been blocked (or returns blocked funds).	Wrong obligation chosen at the teller/operations layer.	Train operations on block-vs-reject; build it into payment controls (§ 3.1).
Reliance on a general license without meeting every condition.	GL is self-executing only if all conditions are met.	Document the condition-by-condition fit before relying on any GL (§ 6.2).
Stripping or omitting sanctions-relevant data from payment messages.	Defeats screening; treated as willful/egregious.	Never alter payment data to avoid screening — a fast track to criminal referral.

CRITICAL — STRICT LIABILITY MEANS "WE DIDN'T KNOW" IS NOT A DEFENSE

Because civil liability does not require intent, the absence of knowledge does not prevent a violation — it only bears on the penalty. The protective measures are upstream (a real risk-based SCP) and downstream (prompt blocking/reporting and voluntary self-disclosure), not a good-faith argument after the fact.

KEY COMPLIANCE TAKEAWAY

Assume strict liability, prevent through the five-component SCP, and if a violation surfaces, preserve mitigation by acting on it immediately and considering a voluntary self-disclosure.

10. Key FAQs

Operative answers to the cross-cutting FAQs referenced inline above. These are OFAC's foundational, program-neutral FAQs; program-specific FAQs are catalogued at OFAC's FAQ index.

FAQ #7 — **How can I engage in a transaction that OFAC otherwise prohibits?**

Through an authorization. General licenses are self-executing for anyone meeting their terms; some activity is statutorily exempt (personal communications, information, travel-incident transactions); otherwise apply for a specific license. A non-U.S. person generally does not risk sanctions for activity a U.S. person could do without a license.

FAQ #74 — **What is a license, and what are the two types?**

A license is OFAC authorization for an otherwise-prohibited transaction. A general license authorizes a class of transactions for all who meet its conditions, with no application. A specific license is issued to a named applicant for a named transaction on application. All conditions must be strictly observed.

FAQ #127 — **When must property be blocked rather than rejected?**

If a blocked person has an interest in the property, the U.S. person must block (freeze and hold) it unless a license or exemption authorizes rejecting or processing it. Where blocking is not required (e.g., a prohibited dealing without a blocked party's property interest), the transaction is generally rejected and returned.

FAQ #369 — **What does the Sanctions List Search tool cover?**
It searches both the SDN List and the Consolidated (Non-SDN) lists and shows, under the List column, which list a potential match appears on — so the user can determine the applicable legal consequence.

FAQ #399 — **Does OFAC aggregate the stakes of multiple blocked persons under the 50% Rule?**
Yes. Ownership of 50% or more in the aggregate by one or more blocked persons makes an entity blocked. A 25% stake held by one blocked person plus a 25% stake held by another results in a blocked entity, and stakes held under different OFAC programs are aggregated.

FAQ #401 — **How does the 50% Rule treat indirect (layered) ownership?**
"Indirectly" refers to ownership through one or more intermediate entities that are themselves 50%-or-more owned in the aggregate by blocked persons. Such layered ownership chains result in blocking down the chain; OFAC urges caution with complex structures.

FAQ #422 — **How do I obtain OFAC's lists other than the SDN List?**
The non-SDN lists are disseminated together as the Consolidated Sanctions List data file; human-readable versions and details are on OFAC's Additional Sanctions Lists page. Names may also appear on the SDN List where a blocking provision attaches.

FAQ #751 — **Should I seek a specific license if a general license already covers me?**
No. It is OFAC's policy not to grant specific licenses for transactions authorized by an outstanding general license (see 31 CFR § 501.801(a)). Rely on the general license and document that its conditions are met.

FAQ #1196 — **What if I blocked and reported property by mistake?**
Property blocked due to mistaken identity or typographical error may be unblocked and an unblocking report filed under 31 CFR § 501.603(b)(3), citing FAQ 1196. Unblocking property in which a blocked person actually has an interest, without OFAC authorization, exposes the U.S. person to penalties.

11. Official Document Index

Statutes

- International Emergency Economic Powers Act (IEEPA), 50 U.S.C. §§ 1701–1706
- National Emergencies Act (NEA), 50 U.S.C. §§ 1601–1651
- Trading with the Enemy Act (TWEA), 50 U.S.C. §§ 4301–4341

Regulations (31 CFR Chapter V)

- 31 CFR Part 501 — Reporting, Procedures and Penalties Regulations
- 31 CFR § 501.601 — Records and recordkeeping requirements
- 31 CFR § 501.602 — Reports to be furnished on demand
- 31 CFR § 501.801 — Licensing procedures
- 31 CFR Part 501, Appendix A — Economic Sanctions Enforcement Guidelines

Guidance

- A Framework for OFAC Compliance Commitments (May 2, 2019)
- Revised Guidance on Entities Owned by Blocked Persons — the 50% Rule (Aug. 13, 2014)

Lists and tools

- OFAC Sanctions List Search
- Sanctions List Service (SLS) — downloads

- Additional (Non-SDN) Sanctions Lists

OFAC pages

- OFAC home
- Sanctions Programs and Country Information
- OFAC License Application Page
- Frequently Asked Questions (all FAQs)
