# Government Investigations

## Under Fire in a Mega–Trade Sanctions Case

TRIP MACKINTOSH

**The author is a partner at Holland & Hart LLP, Denver.**

Imagine you get the call. Agents are in your client's company, taking documents, computers, machining tools, and anything else that stores data. The warrant alleges violations of trade sanctions with Iran or export controls on munitions and dual-use technologies.

We've been there and we sympathize. We have seen it all firsthand: multi-agency investigations with tight deadlines, a parallel criminal investigation, threatened debarment or denial of export privileges, and numerous teams of counsel working in tandem on different aspects of the defense.

We have been in the middle of expansive litigation and had to take responsibility for producing and managing sophisticated, responsive protocols and practices that included means for coordinating with other specialty counsel, sharing key data and documents, and developing proactive regulatory responses to forestall adverse action by regulators. Our representations have included criminal and civil enforcement actions involving satellite manufacturers, providers of security services in Iraq and Afghanistan, high-technology companies supporting complex defense systems, and global aerospace firms.

With the benefit of hindsight and the luxury of time for reflection, let's examine some key aspects of this complex experience. Although the insights may appear self-evident in the calm, they easily get lost somehow in the rush of multifaceted litigation.

Let's say your client calls to tell you that catastrophe has struck. Immigration and Customs Enforcement (ICE) detained your client's non-U.S. executive before allowing him to pass through U.S. Customs and Border Protection. You are not sure what he has reported, but he left the interview shaken.

He had no counsel. He cannot remember all the questions, but they had to do with an export of a particular product. He said the agents asked why he would have allowed the unlicensed export of an item known to be controlled by the International Traffic in Arms Regulations (ITAR). The more questions he answered, the worse it seemed to get.

As counsel, you do not know the scope of the problem—only that the federal authorities have identified apparent violations. It seems obvious that the government is reviewing your client's imports, exports, and executive travel. Where there is one compliance lapse, you understand there may be others.

Later that day you watch the news. You see a report of a coordinated ICE and Federal Bureau of Investigation (FBI) raid of your client's offices. The images are compelling and familiar: lots of agents carrying lots of boxes and equipment to a large tractor trailer.

Published in *Litigation*, Volume 38, Number 3, Spring 2012. 

Then you get the expected call from the in-house general counsel. The company is at a virtual standstill. It needs its equipment back, its data returned, and, of course, an immediate assessment of the nature and scope of the problem.

The warrant application, kindly provided by the Assistant U.S. Attorney, states that "ITAR-controlled data have been exported to China." To the nonspecialist general counsel, this does not indicate the severity of the problem.

Of course, we all know that the easiest entry point for counsel is early on, when there is an inkling of trouble, when you can cobble together a plan of (compliance) action and can keep the problem contained. But this clearly isn't one of those instances.

Regardless of where one enters, there are some critical first steps that should prove beneficial, regardless of the regulations or underlying statutes grounding the investigation.

Our matters have involved export controls and trade sanctions; yours may be prompted by environmental or labor investigations or by an industrial accident. In all cases, however, the same set of litigation management tactics comes into play.

As in other areas of federal law enforcement, export enforcement actions routinely involve multiple agencies working simultaneously (and, sometimes, even harmoniously) in pursuit of different, but related, public policy goals.

Walking in as defense counsel for a company under investigation for trade sanction violations, across the table (and often with subpoena in hand) you typically find agents from ICE, the FBI, the Defense Criminal Investigative Service (DCIS), or similar "transnational" agencies investigating activities governed by overlapping regulatory regimes.

It should go without saying that counsel primarily experienced in the relatively well-trod areas of the criminal law (that is, Title 18 of the U.S. Code) should step carefully when approaching trade sanctions issues for the first time. Unlike other areas of criminal enforcement, trade sanctions matters involve multiple and overlapping regulations, which make them both unique and uniquely knotty.

Illustration by Nigel Buchanan

Trade matters, in fact, have their own particular alphabet. If the business conduct involves defense trade—including weapons systems, components, training, or services—the ITAR apply.

The ITAR, enforced by the State Department's Directorate of Defense Trade Controls (DDTC), emanate from the Arms Export Control Act and, in general terms, with some narrow exemptions, provide that certain defense and military-related technologies may be shared only with explicit State Department permission. If the ITAR do not apply, trade of "dual-use items" (i.e., commercial items with potential military or defensive application) is subject to the Commerce Department Export Administration Regulations (EAR).

The Bureau of Industry and Security (BIS) at the Commerce Department is, in turn, responsible for enforcing the EAR. The empowering statute is the International Economic Emergency Powers Act.

Whether ITAR-controlled or EAR-controlled, all international transactions fall within the scope of regulations issued by the U.S. Treasury Department Office of Foreign Assets Control (OFAC).

The OFAC regulations contain the country-specific sanctions, such as the embargoes against perpetual non-U.S.-friends—Myanmar, Iran, Sudan, Syria, and Cuba—as well as sanctions against individuals, including identified narco-terrorists, Islamic terrorists, and supporters of embargoed regimes.

These restrictions apply regardless of the level of technology involved, whether a radar system or a desk chair, bomb, or bed. Except for the historic Cuban sanctions, these restrictions come from the statutory authority of the International Economic Emergency Powers Act.

The Departments of State, Commerce, and Treasury produce lengthy lists of debarred, denied, or prohibited parties. Absent specific licensing, trade with any of these parties is not allowed.

Violations of the regulatory regimes can result in serious criminal and administrative penalties. ITAR violations, for example, can result in felony sanctions of up to 10 years in prison, criminal penalties of up to $1 million per violation, and civil penalties of up to $500,000 per violation.

"Willful" EAR violations, in turn, carry a "per violation" penalty of $1 million, but can also result in a 10-year maximum sentence (whereas "knowing" violations carry lesser sanctions). OFAC criminal sanctions include a potential stiff sentence of up to 20 years of imprisonment.

In addition to these sanctions, debarment from government contracting, loss of export privileges, and revocation of issued licenses are all part of the government's beefed-up enforcement arsenal.

A company active in international commerce that makes errors in trade controls can quickly rack up scores of violations and massive potential penalties.

Enforcement of these criminal laws is often a combined effort of the individual U.S. Attorney's Office and lawyers from the Department of Justice, National Security Division, Counterespionage Section.

Civil and criminal enforcement can involve any one of many agencies, including the DDTC; BIS; the Department of Homeland Security; ICE; the FBI; and the Bureau of Alcohol, Tobacco, Firearms and Explosives.

All this means that the government will have specialists who know the regulatory regimes. The defense, accordingly, should be similarly equipped.

Suffice it to say that white-collar counsel can be brought in at all points in export enforcement matters. The focus here is on trade sanctions, but multidimensional enforcement matters can emanate from state or federal authorities dealing with any area of regulated conduct. Those include all aspects of government oversight, from controls relating to financial services, environmental protections, workplace safety, and consumer protection, to regulations involving health care and homeland security.

Enforcement investigations or actions can, likewise, come from a host of angles and for a range of largely unpredictable reasons. Whistleblower reports; searches at borders; competitors; product failures; accidents; chemical spills; "damned journalists"; or the discovery of controlled products, technologies, or people in places they should not be, all can trigger the federal agents' unwelcome knock on the door.

When dealing with multi-jurisdictional trade governed by multifaceted regulatory regimes, the risk that a government actor will become interested and start asking questions rises remarkably.

Here is a checklist of lessons learned, which can be useful regardless of whether one's practice encompasses state or federal level controls and regardless of the subject.

## Create a Workflow Map

Stop the alleged violations by immediately mapping the company's workflow and by issuing directives. As they say, it's not as easy as it seems. Consider the situation you will likely confront. Your client has a business model that is successful. That means that lots of people who work there are doing lots of things involved in the business, while—at the very same time—the federal authorities are examining records and looking for, and finding, potential problems.

Consider that this business model does not have appropriately tailored regulatory "filters" designed to ensure that what

the company is doing is consonant with applicable law. In other words, your client is a typical company that grew first and considered compliance risks second, or maybe not at all.

In some areas of federal or state regulation, prohibitions are a reflection of common sense; the prohibited conduct is patently wrong or evil (or, in the vernacular of academia, is *malum in se*).

## Allowing access to data is the same as exporting data.

Put another way, you don't need a whole lot of training to know that dumping chlorine in the parking lot at night is a bad idea.

On the other hand, if your client makes radar parts for commercial aircraft and gets an order from a military customer for a slight variation, it might not be evident that the innocuous commercial item is now controlled or that your client's mere receipt of an email containing the customer specifications by itself triggered certain restrictions.

In another example, a tire for an F18 aircraft might be an ordinary commercial item, but installing it might constitute the provision of a defense service that activates other laws and for which a license might be required.

Stated plainly, the lines between a controlled export and one that does not have particular requirements are often unclear. And, sadly, common sense does not necessarily apply. Sometimes, the only way to determine which items, technical data, technology, or services are controlled is to conduct a difficult jurisdictional review.

To give you an idea of the *malum prohibitum* nature of these controls, consider this: If the item is ITAR-controlled, you need a license. If the item is EAR-controlled, or "subject to the EAR," you might need a license depending on the technology and the location of the customer. But even if you don't, you might need a license under the EAR (even for a desk chair) if the recipient is engaged in certain activities.

But if the recipient is not engaged in certain activities and the item is not controlled at a particular level, then you do not need a license. That is, you don't need one unless the vendor or another party involved is sanctioned by OFAC; then you do. Clear as mud.

Faced with that sort of non-intuitive scheme, you have to figure out how to convince your client that a review of potential problem areas is urgent and why it is in your client's best interest to put an immediate stop to noncompliant conduct.

General counsel, perhaps unfamiliar with white-collar defense in general and export controls in particular, may bridle at your recommendation. Therefore, you need as solid a basis as possible for convincing the client to do the right thing, right away.

We have learned that certain steps can assist with this process.

In the past, like all good outside counsel, we interviewed executives to learn how business is done, where, by whom, and with whom. We then took that information and implemented measures to stop further violations. Pretty simple, really.

With the benefit of hindsight and review of our multiple export defense efforts, we now believe that a verifiable workflow map of the company, detailing all principal offices, trade lanes, distributors, and contracts, is necessary from the very start. In other words, counsel should produce a comprehensive diagram outlining how the company does what it does, from where, and with whom.

Such workflow mapping stands at the center of the compliance efforts we will discuss next. Therefore, it is critical that the workflow can be verified; it may well be audited later as part of the company's remedial measures.

The workflow map provides a schematic showing where the risks of unauthorized exports (items, data, or services) or transactions with prohibited parties exist in the organization. At the same time, the map provides a basis for understanding the types of exports at issue, their frequency, and their nature.

Counsel then can simply compare the activities represented on the map with licenses, authorizations, applicable exemptions, or exceptions available to the company.

These steps lend support to your request as outside counsel that certain, albeit perhaps profitable, business activities stop immediately, merely to reduce the risk profile. There will almost certainly be some resistance from the business side; after all, much of this ongoing, high-risk conduct is likely entrenched, personnel-intensive, and profitable. Stopping the gravy train will no doubt be disruptive and require persuasive justification.

We, for example, have had to stop deliveries of components for launch vehicles, call off the training of thousands of non-U.S. security personnel in a war zone, and temporarily halt armory services at forward-operating bases in Afghanistan. Clearly, you have to have a legitimate basis for that sort of disruption.

Hitting the brakes on client business activities probably will also implicate the client's contractual responsibilities and, in some cases, the security of U.S. or other personnel. Therefore, a directive to stop such conduct must be both necessary and defensible.

Of course, any instruction that results in an interruption likely will not enjoy privilege and, indeed, may later be part of a presentation to federal authorities about the company's

remedial efforts. Therefore, any written directive needs to be drafted to emphasize the importance of the underlying government policy, the specific compliance requested, and the need to stop unauthorized conduct. You should determine the content of the directive and the personnel who receive it in the context of the workflow mapping and the regulatory analysis that will identify points of potential violations.

At the same time, it is imperative to preserve relevant records. This is easier today, as most companies have data flowing through central servers. One challenge in export cases, however, is that data may be held in remote or difficult-to-access locations involving, for example, computers of non-U.S. employees or hard-copy records kept overseas.

The workflow map is designed to facilitate a targeted preservation effort. Preservation of data and a preliminary mapping of where those data reside are, after all, important first steps in any defensive effort.

This preliminary regulatory assessment may help avoid a problem particular to export cases. It is common that information technology (IT) administrators are either visa-holders working in the United States or even non-U.S. nationals located outside the country. Under U.S. export control laws, those persons are "foreign persons," whether located in the United States or elsewhere.

Export of data to those persons may well require licensing, because allowing access to data is the same as exporting data. Those foreign persons, therefore, cannot have access, even theoretical access, to certain controlled data.

If you were to issue a directive to an IT administrator to preserve data, and exporting those data to the IT administrator itself poses a problem, you would inadvertently be complicating the company's remedial workout. You can avoid that pitfall by using the recommended preliminary workflow analysis to do a regulatory assessment.

## Open the Silos

Enforcement matters of the type we are addressing may involve specialty corporate, government contracting, criminal, and regulatory counsel. All those specialty counsel interface with the company, normally through the general counsel. Each counsel will have different key tasks and, accordingly, different priorities and government points of contact.

Here, again, our experiences may be instructive. More than once, we have been brought into export enforcement actions in which the company already has engaged corporate counsel, a local criminal firm to deal with the U.S. Attorney's Office, specialist counsel charged with responsibility for government contracts, and separate counsel for key executives.

Counsel in our position are expected to craft a solution that incorporates all those players. They often are, however, effectively "siloed" by their specialties and specific responsibilities. It is usually the responsibility of one lawyer or set of lawyers to open the silos for the company's long-term advantage, to achieve a consistent, coordinated response from the company that incorporates input from all counsel.

Here's an example: Outside counsel's export analysis concludes that certain conduct—let's say supplying of a product or training—must cease. Meanwhile, corporate or contract counsel determines that cessation of the conduct threatens to trigger breach of contract charges and other adverse consequences. And criminal counsel, for its part, frets that the manner of stopping the conduct will have an adverse impact on the company's presentation to the authorities of its compliance and remediation efforts. Employment counsel notes that stopping the conduct will have a disproportionate impact on protected classes of employees and contravene other legal protections.

To help alleviate these concerns, all counsel need to be able to access—via a shared database or an extranet—the full range of relevant analyses, business-flow maps, lists of authorizations, and copies of compliance documents.

In this regard, our experience is that, before establishing a secure shared database or extranet, counsel need to address the following:

- terms of access and security credentials;
- a general map or layout of the site created with input from all counsel on the categories of data they will be providing;
- requirements, applicable to all counsel, about the data to be posted (for example, that the materials include all submissions and correspondence to government agencies, all substantial work product, and the like);
- a government contact roster to be converted into a chronology and summary of all government contacts;
- an ongoing "chron file" of all submissions from all counsel (we frequently see that, by the time one counsel is resolving the matter, others have closed out their work on which that counsel needs to rely);
- a plan for "sub-extranets" for certain counsel (such as those representing individuals) who will need access to some but not all of the extranet content;
- a task-tracking application to assist in the management of the project and setting of priorities;
- e-discovery software, agreed upon in advance, with shared instructions as to how to craft search terms;
- contacts for technical support; and
- methods to police counsels' collective participation in this extranet to avoid continuation of a silo approach (there is, after all, a clear tendency to continue to act independently

and on one's own, even after this group-coordination mechanism is in place).

## Develop a Culture of Compliance

Agree on a plan that reflects triage analysis and shared information. Now that you have engaged your colleagues, you can begin a multivariate analysis of different legal risk areas, how they intersect, and how they lead to a combined strategy that puts the company in the best possible position. The goal should be to address or remediate any criminal exposure and then deal with administrative or contractual risks in descending order of possible adverse consequences.

Acknowledge the regulatory imperative. Trade sanctions are generally designed to keep controlled technologies, know-how, or money from those who engage in terrorism or would develop or proliferate weapons of mass destruction or their delivery systems. They also support other key national security and foreign policy goals, such as the sanctioning of a repressive or dangerous government or group.

If a company does not have a compliance system that reflects the importance of those controls, it will need to put such a program in place prior to resolution of the enforcement action. To move the company in the right direction and to signal to regulators that the company truly understands the larger policy, a natural first step is to endorse the importance of the controls.

That means that the company has to develop a bona fide top-down commitment to a culture of compliance. This will, of course, be a great benefit when counsel discusses possible resolution with regulators.

To demonstrate that the company endorses these policy imperatives, the first step is thus demonstrable and genuine compliance.

In terms of guidance on how to achieve these objectives, U.S. Sentencing Guideline 8B2.1 provides a minimum expression of what the compliance response should contain. Department of Justice prosecution guidelines describe the factors the department considers when deciding to charge an entity, key among them being the competence of the compliance controls. Each of the agencies with trade sanction jurisdiction has published best practices or compliance guidelines. These need to be integrated into the compliance design.

Whatever compliance solution is best, it has to be designed to produce, as soon as possible, data that confirm that the company is operating in a compliant manner. Those data would demonstrate empirically that the controls are working from beginning to end of contract performance, export transactions, or other conduct. These data become important proof of compliance as well as crucial pieces of evidence for the defense effort.

Training is a key to compliance. By the time the company is in the midst of an enforcement procedure, its credibility has been harmed, if for no other reason than because it is being investigated. Therefore, counsel has to demonstrate to regulators that operational personnel understand compliance requirements and will abide by them. This allows regulators to move forward in a positive direction, even though they may have lingering suspicions about management.

Demonstrate that understanding is achieved through training on the compliance controls mentioned above. But it is of no value to have training without proof—empirical data—that the employees understand their obligations under the regulations. Without more, sign-in sheets and PowerPoint slides indicate merely a possibility that the training was effective (and a mere possibility, in many cases, can hurt the company's efforts to appease the authorities).

> Export cases can result in immediate government sanctions.

In trade enforcement actions, for example, it is often preferable to have web-based content and training tailored to the company's activities. Trainees should be tested and monitored. This means that the training vehicle needs to be able to track who logged in, for how long, and from which destination.

Our experience is that this sort of training, when implemented company-wide, is the most efficient and has the most impact. Face-to-face training, with its important potential for real dialogue, should complement web-based instruction.

Collaborative discussions among counsel should inform the development of the training platform, content, and data grabs (empirical evidence of effective training). For example, criminal counsel should be able to offer particular scenarios or hypotheticals in light of their review of the company's conduct. Similarly, regulatory counsel may have other concerns that would be reflected differently in the training content.

The ultimate goal is to have a legitimate basis for telling the government that the company now has internal guardians of compliance; namely, the employees. The more that training addresses the government's concerns, the better. To know where the points of failure were with respect to multiple legal areas, you need to have collaborative contribution by all counsel.

Export cases can result in immediate, and often debilitating, government sanctions. The State and Commerce Departments have authority to enjoin conduct pending resolution of the

issues. Both State and Commerce, moreover, can issue orders revoking previously issued licenses, barring the party from any further exports, or both.

These actions normally are taken when the government believes they are necessary for national security or foreign policy reasons. In addition, agencies in charge of government contracting have suspension and debarment authority and can take adverse and preemptive action, sometimes disqualifying a company from contracting altogether. That sort of action can doom a company.

Looking forward, if the company is found to have violated the law and it engages in a settlement with either State or Commerce, a likely condition of that settlement would be a special compliance monitor. That monitor typically would oversee the company's post-settlement remedial responses and compliance.

Because the end game may result in the imposition of a monitor and an improved compliance system, and because there is a risk that the government might act precipitously, preemptive action is the call of the day.

The key elements of a response would be:

- public acknowledgment of the importance of controls;
- demonstration of the company's commitment to compliance;
- creation or improvement of the compliance system in response to the enforcement action; and
- creation of an independent committee or other authority to monitor compliance during the enforcement period.

If the independent oversight committee has appropriate authority, the agencies may take that into account. In one remarkable instance, the State Department, in lieu of imposing its own monitoring, adopted a company's independent export control oversight authority into its action plan. This allowed the company to rely on its own controls and avoid having the State Department conduct an event-by-event analysis and potentially deny license applications.

If an independent regulatory oversight authority (a sort of "regulatory receiver") is put in place, the mandate of that authority should be consonant with the strategies of criminal counsel as well as the strategies of the several civil counsel. This means, of course, that counsel will be working together to establish how the new authority will function.

The benefit of a regulatory receiver may be most evident when resolving matters with the Department of Justice. Therefore, details of that authority need to be vetted by counsel responsible for criminal representation. The same applies to other federal authorities that might examine the receivership, such as the suspension and debarment offices of the contracting agency. You should have criminal counsel provide input on what the special authority or receiver should look like to meet anticipated concerns of other federal agencies.

An independent regulatory receiver should have authority to

- inquire about any export transaction,
- stop any transaction,
- report directly to federal or other agencies,
- cause outside counsel to investigate transactions or related conduct, and
- report directly to company ownership or management.

The mandate should require the independent authority to maintain a detailed docket of all its "official" actions. Directives from the authority should be numbered and made part of this docket, as should all communications with regulators. Meeting minutes and other correspondence also should be part of the file. All of this will form a substantial component of the company's remedial response as the matter moves through different agencies for review.

## Lessons Learned

Vernon Sanders Law noted, "Experience is a hard teacher because she gives the test first and lessons afterwards."

As we have seen, complex trade sanctions matters share many attributes with other multifaceted regulatory enforcement actions, requiring counsel to balance interlocking regulatory and enforcement regimes while dealing with critical time constraints.

Key objectives for counsel handling any multi-agency matter are to stop ongoing violations, ensure lateral communication with counsel and the client, and develop a strategic response that incorporates proper remediation, mitigation, and compliance.

In an environment in which a backdrop of national security and foreign policy issues and concerns drive the analysis and the authorities' expectations, companies must be prepared to deliver the highest standard of response and remediation. As we have learned the hard way, those steps are not as easy as they might appear.

Although enduring an enforcement procedure is never pleasant, one sure thing is that everyone on the company side who went through it will remember who helped solve the problems and who simply compounded the pain. We hope our insights will help put you in the former category. ■