Foreign Duty: Export Control Goes Private

Anne Proffitt Dupre

University of Georgia School of Law, adupre@uga.edu
If you’re an exporter, it pays to be a know-it-all these days. Does there appear to be even a slight potential that the item you’re shipping could play any part at all in modern weaponry? Then you need to know exactly how that item will or may be used. You also may need to know who will ultimately use it, and where.

If you’re a lawyer advising either that exporter or a supporting financial institution, you, too, now need an extra measure of vigilance. For one thing, it helps to know how to write loan documents with the necessary safeguards to cover possible violations of the recent government regulation that requires so many people to be in the know.

The regulation that is introducing this new era for exporters is the year-old Enhanced Proliferation Control Initiative (EPCI). It seeks to control the spread of nuclear, chemical and biological weapons and missile technology by “privatizing” the monitoring of exports. With this approach, the government is essentially shifting the responsibility away from itself and onto industry for keeping close watch over shipments of products and technologies.

Whether a business ships something serious, such as sensitive computer software, or innocuous, such as paper clips, it must adhere to the EPCI—and the government is talking tough about penalties for violators.

What changes does the EPCI require of businesses involved either directly or indirectly in exporting? And how should lawyers who represent those businesses change their methods?

This article will spell out the sorts of internal changes—compliance supervisors, for example—that businesses need to introduce. It will also take note of the need for the lawyer to adapt loan agreements with EPCI compliance in mind, and to review an exporter’s principal agreements.

Just say ‘know’

The U.S. Department of Commerce late in 1991 began to implement the EPCI, which imposes new and expanded controls of unprecedented scope. Exporters of commodities or technical data (including software) need to pay close attention to EPCI’s power.

Indeed, it will be difficult for them not to pay attention: In its arsenal of weapons to enforce the EPCI, the government can deny a violator export privileges, impose a fine of up to $1 million or imprison the violator for up to 10 years. Pending legislation would double the latter two penalties.

EPCI requires an individual validated license for the export, re-ex-
port or transfer of any commodity or technical data that the exporter "knows," "has reason to know" or "is informed" is destined for a prohibited nuclear, chemical or biological weapons or missile development end use or end user.

EPCI thus imposes on all U.S. exporters a "know-your-customer" rule. Significantly, knowledge by an employee will be imputed to the employer.

EPCI's prohibitions extend not merely to sensitive weapons-related technology but also to any commodity, including those items that are not otherwise subject to control, which the exporter "knows" or "has reason to know" might have a prohibited end use. Thus, because the new export controls cover seemingly innocuous items like paper clips and rubber bands, exporters must assume greater care for items that would normally be eligible for general licenses.

Put simply, EPCI demands that exporters and their employees know what and to whom they are selling, as well as where the exported item is going—and why.

Furthermore, EPCI's controls have an extraterritorial reach that applies to U.S. citizens or permanent residents anywhere in the world. EPCI applies to: 1) direct branches (but not subsidiaries) of U.S. companies outside the United States, and 2) U.S. citizens and permanent residents wherever they are located.

Although foreign subsidiaries are not covered by EPCI, if a subsidiary is staffed by a U.S. citizen or permanent resident, its activities may be covered by EPCI. This is of particular significance because the extraterritorial reach of EPCI covers re-exports and transfers regardless of origin of the goods or technology.

Thus, a U.S. person abroad who transfers wholly non-U.S. products outside the United States is covered by the regulation. This type of personal jurisdiction is a major departure from past practice. Until now, the U.S. Export Administration's regulations applied solely to U.S.-origin goods or technical data.

In this new staging of the export-control drama, with the government as revising playwright, the government's reach extends far—down even to the sublayers of an exporter's supporting cast of characters.

The EPCI prohibits U.S. citizens and permanent residents from knowingly "supporting" an export, re-export or transfer that does not have a validated license if one is required. The EPCI regulations define "support" as "any action" that "facilitates" the transaction, including financing, transportation and freight forwarding.

In addition, EPCI prohibits U.S. citizens and permanent residents from knowingly performing any contract, service or employment that will "assist" chemical or biological weapon or missile activities. The plain language of the regulation thus appears to include even the lawyer for a financial institution, or the lawyer for a transportation or freight-forwarding company who helps with such transactions.

Certainly, U.S. financial institutions and their foreign branches are at risk of violating EPCI. They therefore will need to monitor the identities of their customers and the nature and destinations of their customers' products.

What about the lawyers for those financial institutions? They should redraft standardized loan agreements to include indemnity clauses governing liability for EPCI violations. Loan documents may also be redrafted to include the requirement of additional documentation so that a financial institution assures itself of the innocence of its customers' dealings.

Devising a game plan
Because the Commerce Department recently has made it clear that EPCI will be an enforcement priority, it is imperative that each U.S. exporter have in place a much more extensive internal control program (ICP) than the type that would be sufficient for a bank.

Overseeing the ICP is the person known as the compliance supervisor, who is responsible for monitoring indications of suspicious transactions. In general, the compliance supervisor should be responsible for monitoring all exports that the exporter knows might have a nuclear, chemical or biological weapons or missile development end use. The compliance supervisor also needs to monitor all related agreements, invoices and shipping documents.

If an exporter is located outside the United States, the compliance supervisor should screen all transactions by which the exporter buys commodities or technical data from this country for delivery across national borders. The compliance supervisor should also monitor all training and sales programs here that involve foreign nationals, as well as sales trips abroad that might result in an indirect "export."

The compliance supervisor should be responsible for developing and updating effective screens for nuclear, chemical and biological weapons and missile development end users and end uses. These screens need to be individually tailored. It is important that the compliance supervisor know all applicable regulations in order to distinguish among the different licensing requirements governing each end use.

But self-education is not enough for the compliance supervisor. He or she is also responsible for educating each employee, because an employee's knowledge will be imputed to the employer/exporter. The compliance supervisor should encourage employees to report anything suspicious about an end user.

When red flags wave
Certain informal guidelines defining suspicious circumstances are

Dupre is an associate at Shaw, Pittman, Potts & Trowbridge in Washington, D.C.
available from the Commerce Department. The guidelines, referred to as “red flags,” require an exporter to focus on any unusual circumstances that could indicate the exported item may be destined for an inappropriate end use or end user. If an exporter or any of its employees sees a “red flag,” the exporter has a duty to investigate before continuing with the transaction. An exporter may not ignore “red flags” or avoid asking necessary questions of a customer.

For example, if an exporter of computers normally installs the hardware and maintains it for a certain time, but the customer avoids those customary services, then the exporter has a duty to investigate the customer’s reasons before continuing with the transaction. Similarly, the presence of an end-user on the Commerce Department’s published denial list is a bar to the transaction. The federal agency will soon publish a more formal list of “red flags.”

Before an exporter who sees a “red flag” takes any action such as canceling contracts with a customer, the exporter should consult its lawyer. Some “red flags” can appear in innocent transactions. For example, sometimes a contractor in a normal commercial setting may refuse an exporter access to a portion of its plant unconnected to the transaction. Therefore, as it tries to avoid EPCI liability, the exporter needs to exercise careful judgment—or it might find itself in court defending itself against a breach of contract action.

The lawyer’s role

An exporter’s lawyers, those both in-house and outside, should be involved in several other aspects of an internal control program. For instance, each exporter needs to fashion a policy statement regarding export controls. The exporter should update and redistribute the statement to all employees whenever there are changes in the ICP or in EPCI laws and regulations. Large exporters should bring in outside counsel to review the ICP independently.

Additionally, lawyers should review all of the exporter’s principal agreements. Purchase and sales orders, and agreements for distribution, training, joint venture and technical assistance should be redrafted to contain contract provisions allocating the responsibilities and obligations created by EPCI. Similarly, destination-control statements should be drafted and added to air bills and bills of lading.

No guarantees

If an exporter conscientiously complies with all of the suggested internal regulatory steps, will it be protected if a violation of EPCI occurs?

The answer is no; there are no safe harbors under EPCI. It is obvious, for example, that liability will apply to the U.S. exporter who deals in missile technology software with Iraq. But it will apply with equal force to the U.S. bank that finances shipments of foreign-manufactured widgets to a country on the Commerce Department’s list if the bank has reason to know that such widgets could be bound for a prohibited end use.

Therefore, it is clear that EPCI will impose new and significant responsibilities on exporters, as well as on financial institutions and others who deal with exporters. All companies at risk of violating EPCI must formulate clear policies regarding EPCI compliance and establish export-management systems that will help reduce the risk of inadvertent violations.

And all agreements should be reviewed to ensure that financial liability is appropriately allocated in the event that the business inadvertently runs afoul of this more demanding system.

---

But when a lawyer does speak, it must be with style and passion. In the practical heart of the book, an essay entitled “From Jefferson to the Gul’ ‘ar: How Lawyers Have Lost Their Golden Tongues,” Weisberg blames the passive voice for the growing disenchantment with legal discourse. He predicts that lawyers will recover their true professional power and self-respect only when they have reclaimed their speech from passivity, redundancy and weak verbs.

Thus, “the first step to professional bliss lies, once again, on the path to strong syntax. The lesson is brief and deceptively simple: Choose the best subject, grammatically speaking, for the sentence.” That subject can even be oneself: Lawyers, who “are in truth a modest lot,” should use the first-person singular in making recommendations at the end of memoranda. Finally, lawyers should read “at least one novel a month.”

Just as effective writers adhere to the rules of grammar and style, so should the legal community appreciate the fundamental moral principles underlying specific statutes. Finally, judges and lawyers should broaden their life experiences in addition to their reading lists.

And perhaps thus, as Poethics promises, “to the twin satisfactions of mastering a procedural environment and standing for the last discernible (if still relative) values, the lawyer can add the quiet reward of an artistic job well done.”

ABA SECTION OF BUSINESS LAW 49