

## Is Your Export Compliance Plan Up to Date? Implementing Adequate Controls That Address Current Technology

*Suzanne D. Reifman and Amanda J. Dietrick, Vinson & Elkins L.L.P.*

Today we are inundated with media accounts about the dangers of cell phones, text messages, Facebook and the like. Stories frequently warn of the need for parents, in particular, to remain current with the latest technology and implement appropriate "parental controls." The same general principle applies to developing and administering an export compliance plan. In most cases, unauthorized exports of controlled goods and technology do not occur because employees are intentionally attempting to break the law. Rather, in most cases employees are not fully aware of the ramifications of their actions and do not realize that their communications—now made through a variety of instantaneous methods—could result in export violations. Moreover, all too frequently, there are either no safeguards integrated into a company's business or outdated safeguards, which means that a company often is unaware of possible compliance problems. The purpose of this article is to share our general observations about areas of compliance risk for which we believe companies frequently have not implemented the necessary "parental controls" to ensure they are appropriately monitoring the activities of their employees. This applies both to companies with no export compliance plans as well as to companies whose plans simply are not sufficiently up to date to address these emerging risks.

### **U.S. Export Controls and Penalties**

The United States controls the export of goods and technology for national security and foreign policy reasons, primarily under one of the two major export controls regimes. Items specifically designed or modified for military use are regulated by the Department of State, Directorate of Defense Trade Controls (DDTC), under the International Traffic in Arms Regulations (ITAR). Most other items, including commercial items or "dual use" items (those that have both military and commercial applications) are regulated by the Department of Commerce, Bureau of Industry and Security (BIS), under the Export Administration Regulations (EAR).

Failure to obtain a required license or to otherwise comply with the ITAR or EAR can result in substantial fines and penalties. Even for civil violations, penalties under the EAR can reach \$250,000 per violation and penalties under the ITAR can be as high as \$500,000 per violation. Criminal penalties can result in fines as high as \$1,000,000 per violation and imprisonment. Export violations can also result in a number of other draconian measures being imposed, including a loss of export privileges and debarment from government contracting, among others. These penalties do not even consider other consequences, such as interruption of business activities, which can lead to significant commercial repercussions.

---

© 2011 Vinson & Elkins LLP. Originally published by Bloomberg Finance L.P. Bloomberg Law Reports® is a registered trademark and service mark of Bloomberg Finance L.P.

This document and any discussions set forth herein are for informational purposes only, and should not be construed as legal advice, which has to be addressed to particular facts and circumstances involved in any given situation. Review or use of the document and any discussions does not create an attorney-client relationship with the author or publisher. To the extent that this document may contain suggested provisions, they will require modification to suit a particular transaction, jurisdiction or situation. Please consult with an attorney with the appropriate level of experience if you have any questions. Any tax information contained in the document or discussions is not intended to be used, and cannot be used, for purposes of avoiding penalties imposed under the United States Internal Revenue Code. Any opinions expressed are those of the author. Bloomberg Finance L.P. and its affiliated entities do not take responsibility for the content in this document or discussions and do not make any representation or warranty as to their completeness or accuracy.

## Key Elements of an Export Compliance Program

As a result of these penalties, which can cause incalculable harm to the company and its employees, it is essential that companies implement an effective compliance program to guard against the possibility of violations. Both BIS<sup>1</sup> and DDTC<sup>2</sup> provide general guidelines on their websites for establishing compliance programs. At a minimum, a compliance plan should address the following:

- Management commitment to export compliance;
- Personnel designated to monitor and facilitate export licensing and compliance on a day-to-day basis;
- Procedures for determining export jurisdiction and classification of products and related technology to identify applicable controls;
- Procedures for identifying applicable export authorization and reporting requirements; preparing and submitting export license applications; and properly administering government license approvals;
- Screening for export controls purposes, to ensure the company is not doing business with any ineligible or sanctioned parties or persons;
- Procedures for controlling exports (particularly those involving technology) to foreign persons, including foreign employees, contractors, and visitors;
- Recordkeeping;
- Periodic training of employees on export compliance;
- Monitoring and auditing for compliance; and
- Procedures for handling and disclosing violations, including employee disciplinary action.

Notwithstanding these general categories, just as parental controls must be dynamic to accommodate emerging technology, export control processes also must change as necessary to address new

compliance risks. While almost any export compliance plan is better than no compliance plan, for many companies, such plans essentially consist of a series of aging policies and procedures that are gathering dust on a shelf. As a result, it has been our experience that the following areas tend to be problems for companies that have plans, as well as for those that do not have them.

## Recommended Areas for Updated Controls

### — Hardware Exports: "Where is it Going . . . and When is it Coming Back?"

Customers continually demand smaller and smaller equipment, in virtually all industries. As a result, the ability to track exports of these items has become more and more challenging. In the past it was likely that an employee would have to enlist the assistance of the company's shipping department to package and transport equipment, especially to foreign locations. However, in many industries, employees can now simply slip their widget into an envelope and export the item without assistance from virtually any location (especially if they have the company's Federal Express or other courier account number). As a result, for many companies, a compliance plan that assumes its shipping department will serve as the gatekeeper for hardware exports and does not address exports made by other means may be woefully out of step with current shipping practices.

Similarly, the increased demand for and supply of smaller equipment creates compliance challenges for companies who need to ensure the return of temporary exports. A bailment or consignment period of one year or more might have been workable in years past, when equipment was large and likely could only be used by limited companies or individuals. However, today, equipment can more easily be re-exported or lost by foreign recipients. This means that for many companies, today's compliance plans need to include tighter restrictions on consigned goods and shorter consignment periods, among other things.

Companies that rely on inventory management systems to track hardware should take special care to ensure that they effectively incorporate export controls. Although some systems are designed to flag "foreign" shipments to ensure that the company has obtained the necessary export license, in some cases a shipment outside of the United States may not be designated as "foreign" if the order was placed by a U.S. sales office or through a U.S. distributor. Similarly, a system that is set up to "code" certain products with export classification and jurisdiction information may not work well in practice if companies are now using "Just In Time" inventory management, in which items are shipped to a customer almost immediately after they are received from a supplier. In such instances, it is important that the compliance plan include some effective safeguard for ensuring that these types of items are not exported before they can be evaluated by export personnel.

## — Technology Exports: "Sleep With One Eye Open"

Technology/technical data can be exported through myriad means, including through email, collaborative tools (i.e., FTP site or other file sharing program), and cloud computing services. In addition, technology can be transferred using a variety of different devices, such as home computers, thumb drives, and blackberries. Technology exports can also be made through intangible methods such as via teleconference/videoconference, meeting, plant tours, etc. Companies should consider whether their compliance plans adequately anticipate the methods by which technology may be exported by employees. In too many cases, companies are still relying upon old policies and procedures that pre-date, at the very least, cloud computing and collaborative tools, and assume information is being shipped via hard copy from the mailroom. Additionally, in many cases, policies and procedures do not address the real risks associated with newer methods of technology exports. For example, for exports occurring via email, companies should consider whether it makes sense to "flag" foreign addresses or place controls on the most sensitive

documents to ensure they cannot be simply attached to an email or prompt the sender about whether appropriate export authorizations have been obtained before the email is sent.

With respect to collaborative tools, we find that many compliance plans do not address exports made using this method, even though their employees are routinely using them. If employees use collaborative tools, compliance plans should consider who is authorized to post or delete information and the information that may be posted or deleted. Such procedures should consider who has access to the posted information, and what types of controls are necessary so that foreign persons do not have access without appropriate authorization. This is an area in which personnel handling export compliance issues frequently are not aware of the activities of the IT department and other company functional personnel. Additionally, even in cases where companies are monitoring controls relating to their collaborative tools, there are often no controls on employees posting information to a tool that is used by company personnel but owned/administered by another company.

Export personnel may not be included in business discussions about whether utilizing a cloud computing provider would be beneficial for the company, which creates compliance risk. Although regulatory guidance relating to cloud computing is not fully developed, BIS has issued two advisory opinions that confirm that the cloud provider is not the "exporter of record" and is not responsible for any "deemed exports" that might be made to its foreign employees, suggesting that the companies who use a cloud provider's services need to take appropriate precautions. However, notwithstanding these risks, most export compliance plans do not address exports made using a cloud computing provider.

## — Recordkeeping and Marking: "Enforce Clear and Consistent Rules"

Too often, companies recognize their failure to comply with recordkeeping requirements only after

a violation occurs and they are unable to produce the necessary records. Missing records can quickly become an aggravating factor in an enforcement action and leave an exporter vulnerable to greater civil penalties or even the possibility of criminal penalties. In addition, the number of violations assessed against an exporter can rapidly increase if separate recordkeeping-related violations are charged.

Recordkeeping violations can be minimized by ensuring that a compliance plan spells out, with particularity, which individual(s) is responsible for maintaining export records; which records will be retained; how the records will be retained and in what format; and for what period of time the records will be retained. Simply stating that employees are required to "maintain records" of exports (as we have seen in many compliance plans) is not enough. A workable infrastructure must be established for maintaining the records so that they are easily located, such as in a central folder or database, and properly archived. Failure to establish such an infrastructure can make it extremely difficult to locate records that may be buried in an employee's email inbox or sent box, or impossible to retrieve if such emails become victims of an auto-delete function.

Exports via FTP sites or other collaborative tools pose particular challenges for recordkeeping, especially in cases where the site was not established with export compliance in mind and there is no reliable archive function. For example, some sites are intended to simply allow the one-time transfer of large files and the files are deleted after a brief period, leaving no record of what was exported to whom. In other cases, where multiple individuals have the ability to post and delete information, it is not enough to provide a record of a "final" specification and the date it was posted. The company also must maintain a record of all drafts and related documents that may have been posted (i.e., exported) but deleted at an earlier time. In addition, determining the foreign persons who have access to information posted to a collaborative tool can also be challenging. In cases where company personnel post information to

another company's tool, they frequently have no knowledge of or control over who might have access to their information. Even for tools they administer, we have seen many situations where company personnel, in concert with IT personnel, grant access to other companies or individuals without considering the export compliance implications, with the result that they are unable to conclusively identify the foreign persons who have access to their data at any given time.

Guidance in many company plans regarding marking requirements is frequently as general and as unhelpful as recordkeeping guidance. This would include identifying the control status of a particular document and including the correct destination control statement, as required by the ITAR or the EAR. Compliance plans should not only direct employees to properly mark documents, but also indicate when documents should be marked (at the point of creation, prior to export, etc.), which documents should be marked and how they should be marked. Although we know that many companies have become increasingly sensitive to proper marking in recent years, we continue to routinely see documents that are either not marked as required by the ITAR or EAR or contain rather useless statements, such as "May be export controlled" or "Controlled by the ITAR or the EAR." Even in cases where the documents are not being exported, the use of such confusing markings is likely to create compliance risk by confusing the U.S. suppliers and customers that receive these documents (and possibly making them conclude that it is acceptable for their foreign employees to have access to them).

## — Screening: "Know Who Their Friends Are"

In addition to regulating exports by country, the government prohibits exports to or transactions involving certain entities and individuals. Therefore it is important that exporters establish reliable methods for screening all parties to a transaction to ensure that they do not engage in any prohibited transactions or exports. The government maintains a number of lists of persons and entities that are prohibited from receiving exports. These include

the Specially Designated Nationals (SDN) List, Denied Persons List, Entity List, Debarred Persons List, and Unverified Persons List, among others. Exporters should have a formal procedure in place for screening individuals and companies against all of these lists.

However, screening is an area where we have found that compliance plans often fall short because they fail to give employees adequate direction about how screening should be performed, who should perform it, and how often it should be performed. This creates particular risk, since U.S. sanctions programs are constantly changing and continue to expand in scope (for example, in July 2010, the United States passed into law the Comprehensive Iran Sanctions, Accountability, and Divestment Act, which was specifically designed to reach foreign companies not previously subject to U.S. sanctions who are doing business with Iran). The lists of prohibited persons/entities are updated by the government on an ongoing basis, which means that even if a person/entity is not on a list today, it could be tomorrow. In addition, the SDN List often does not identify individuals who are considered SDNs by virtue of their relationship to a sanctioned person, such as family members of SDNs or entities owned or controlled by SDNs. As a result of these limitations, it may be necessary to conduct due diligence in instances where a party to a transaction could be related to an SDN. Companies should review their screening procedures in order to ensure they take into account the most complete and current information and that screening is accompanied by due diligence where appropriate.

Additionally, because exports can occur at different junctures in the business cycle, companies must also ensure that they are screening at the appropriate times (e.g. at the initial stages of a transaction during marketing or negotiations, or before an item is shipped, etc.).

Finally, a compliance plan must establish the specific steps to be taken when screening identifies a potential "hit" (e.g., an individual or entity is identified as a potential prohibited person or entity). Compliance plans should set forth how

follow-up due diligence will be conducted and who will be responsible for determining whether it is permissible to make exports or have dealings with the individual or entity in question and how appropriate records of any determinations will be maintained.

### — Export Compliance Training: "Keep the Lines of Communication Open"

As stated above, a minimum element of compliance plans includes training of company employees. However, in this age of information overload and continuous communication, companies need to be more thoughtful than ever about the methods of outreach that will be most effective in engaging and informing their employees. We believe that in order to reinforce compliance, an effective compliance plan ideally should promote ongoing interaction with employees, rather than simply relying on employees to read policies and procedures or provide annual or bi-annual training that is easily forgotten. For example, for many companies, rather than focusing on one long annual training course, it may be more beneficial to shorten the annual training, but provide more frequent email updates, brochures, discussions at functional business meetings, or other easy-to-digest guidance that reminds employees of particular areas of compliance risk and changes to export laws and regulations. Finally, in order to ensure that export compliance information is available to employees as they need it, export materials should be available in a location that is easily accessible to employees, such as through a link on an intranet site. This will become increasingly important as U.S. government export reform initiatives continue to be implemented.

### — Export Compliance Audits: "Trust, But Verify"

A required element of an adequate export compliance plan is that it be subject to internal monitoring/auditing. Indeed, effective auditing of a company's export control policies and procedures can be one of the most critical elements in ensuring long-term compliance. Moreover, an increase in

mergers and acquisitions, which can lead to successor liability for the acquiring company, reinforces the importance of a robust audit program. However, in many cases, to the extent audits are performed at all, they do not reach the areas that tend to cause the greatest compliance risk, particularly in cases where exports are made through a variety of technological means and may not be easy to detect. For example, IT systems often are not evaluated to ensure that foreign persons do not have unauthorized access to export controlled information, through collaborative tools or other methods. Similarly, functional processes often are not reviewed to ensure that they are consistent with the company's export compliance plan. For example, a contract with cloud computing service should be reviewed to ensure that it includes appropriate limitations on access by the service's foreign employees. Similarly, Human Resources and Purchasing procedures should be vetted to ensure they have the appropriate controls to prevent unauthorized exports to foreign employees and contractors or to foreign suppliers. In order to identify possible problems in these areas, it is not enough for a company to simply review paperwork relating to export licenses and other documents that evidence the company's compliance with export laws and regulations. Rather, audits need to be sufficiently transactional and conducted with personnel with the appropriate level of subject matter expertise in order to determine whether there are any business transactions for which the company failed to obtain an export license.

\* \* \* \*

A compliance plan that effectively establishes mechanisms for identifying and vetting exports before they occur is critical to avoiding incidences of inadvertent export violations. The key is anticipating when and how exports are likely to occur and to develop processes that are workable in light of a company's business activities. Any such plan should address exports in light of current technology to ensure future compliance.

*Suzanne Reifman is a partner at Vinson & Elkins, LLP in Washington, D.C. who advises clients on the ITAR,*

*EAR, Office of Foreign Assets Control sanctions, and export regulations administered by the Department of Energy and Nuclear Regulatory Commission, among others. Ms. Reifman's comprehensive experience involves training, general counseling, and assistance with export jurisdiction/classification and licensing issues. Ms. Reifman develops compliance plans, investigates instances of noncompliance and prepares disclosures of violations. She also frequently performs M&A due diligence and conducts audits, including audits requested by the U.S. government. Ms. Reifman may be reached at [sreifman@velaw.com](mailto:sreifman@velaw.com) or (202) 639-6577.*

*Amanda Dietrick is an associate at Vinson & Elkins, LLP, in Washington, DC. Ms. Dietrick advises clients on compliance with export controls, economic sanctions, and government contracts regulations. Ms. Dietrick also assists clients with developing compliance plans for exporters, conducting internal audits for export compliance, performing due diligence of export compliance in the context of a merger or acquisition, preparing export license applications, investigating possible export violations, and preparing voluntary disclosures of export violations. Ms. Dietrick may be reached at [adietrick@velaw.com](mailto:adietrick@velaw.com) or (202) 639-6740.*

© 2011 Vinson & Elkins LLP

- 1 U.S. Department of Commerce, Bureau of Industry and Security, <http://www.bis.doc.gov/complianceand enforcement/emcp.htm>.
- 2 U.S. Department of State, Directorate of Defense Trade Controls, <http://www.pmddtc.state.gov/compliance/index.html>.

#### Disclaimer

This document and any discussions set forth herein are for informational purposes only, and should not be construed as legal advice, which has to be

addressed to particular facts and circumstances involved in any given situation. Review or use of the document and any discussions does not create an attorney-client relationship with the author or publisher. To the extent that this document may contain suggested provisions, they will require modification to suit a particular transaction, jurisdiction or situation. Please consult with an attorney with the appropriate level of experience if you have any questions. Any tax information contained in the document or discussions is not intended to be used, and cannot be used, for purposes of avoiding penalties imposed under the United States Internal Revenue Code. Any opinions expressed are those of the author. Bloomberg Finance L.P. and its affiliated entities do not take responsibility for the content in this document or discussions and do not make any representation or warranty as to their completeness or accuracy.