dentons.com

DENTONS

# Insights and Commentary from Dentons

The combination of Dentons US and McKenna Long & Aldridge offers our clients access to 1,100 lawyers and professionals in 21 US locations. Clients inside the US benefit from unrivaled access to markets around the world, and international clients benefit from increased strength and reach across the US.

This document was authored by representatives of McKenna Long & Aldridge prior to our combination's launch and continues to be offered to provide our clients with the information they need to do business in an increasingly complex, interconnected and competitive marketplace.

SEPTEMBER/OCTOBER 2012
VOLUME 18 NUMBER 5

DEVOTED TO INTELLECTUAL PROPERTY LITIGATION & ENFORCEMENT

*Edited by the Law Firm of Grimes & Battersby*

# IP Litigator

Wolters Kluwer
Law & Business

# *US Trade Controls and Cloud Computing*

**Jason M. Silverman**

*Jason M. Silverman focuses his practice on government investigations, export controls, white collar criminal defense, and litigation under the False Claims Act. He also advises clients on matters arising under federal procurement integrity and conflict of interest laws. Mr. Silverman has represented companies and individuals in connection with investigations by agencies of the Departments of Justice, Defense, Commerce and State; the Securities and Exchange Commission; and grand juries.*

Cloud computing is intended to facilitate access to information and expand delivery of services. In contrast, export controls and trade sanctions are intended to restrict the flow of information and limit the provision of goods and services. It is important to understand the legal limitations that these regulatory regimes place on use of the cloud in order to stay within the bounds of the law while fully realizing the promise of cloud computing. This article examines the US export control and trade sanction regimes that may come into play in connection with cloud computing and highlights possible compliance issues for cloud users and providers presented by these regimes.

## United States Export and Trade Controls Regulatory Landscape

The United States employs a dual-track export control regime, which is divided according to the type of goods, technology, or services being exported.[1] On one hand is the International Traffic in Arms Regulations (ITAR), which is administered and enforced by the Directorate of Defense Trade Controls (DDTC) within the Department of State (DOS).[2] The ITAR controls hardware, technology, and services (including software) that are designed for military applications. On the other hand is the Export Administration Regulations (EAR), which is administered by the Bureau of Industry and Security (BIS) within the Department of Commerce (DOC).[3] The EAR controls hardware, technology, and services (including software) that are commercial or "dual-use," meaning used in both commercial and military applications.

The United States also maintains a variety of trade sanctions and embargoes against foreign governments, citizens of certain foreign countries, specified foreign individuals or groups of individuals, or combinations of those categories. These trade sanctions programs generally are administered and enforced by the Office of Foreign Assets Controls (OFAC) within the Department of the Treasury.[4] There is wide variation among the different sanctions programs, and they frequently are modified by executive order. In general, however, these sanctions programs severely limit or prohibit completely many types of transactions with sanctioned entities.

## ITAR Controls

### What Items Does the ITAR Control?

The ITAR controls "defense articles," "technical data," and "defense services," each of which is a defined term in the regulations.

"Defense articles" refers in almost all cases to physical hardware. Technical data and defense services, as the names suggest, refer to intangible technology and services. Physical hardware, obviously, cannot be transmitted via the cloud, while technology and services can. But the definitions of technical data and defense services hinge on whether they relate to a defense article. Understanding how to identify a defense article, therefore, is a critical first step to understanding how ITAR controls relate to cloud computing.

The starting point for the definition of a "defense article" is the US Munitions List (USML).[5] The USML contains 21 categories of items subject to ITAR control. The USML categories include firearms (Category I), guns (Category II), ammunition (Category III), launch vehicles, missiles and bombs (Category IV), naval warships (Category VI), tanks and military vehicles (Category VII), military aircraft and spacecraft (Category VIII), protective personnel equipment (Category X), fire control and optical equipment, including night vision (Category XII), military encryption software (Category XIII); spacecraft systems (Category XV), nuclear weapons (Category XVI), and submersible vessels and oceanographic equipment (Category XX).

Each USML category sets out in general terms the types of items it controls. But the USML is not a positive list

that identifies specific items subject to control. Rather, it identifies types of items that are designed for military application, sometimes by reference to their capabilities or other objective performance characteristics.[6] Under the current definition of defense articles, design intent - whether the item was designed for a military application or purpose - is of paramount importance in determining whether an item is a defense article.

The ITAR is intended to be encompassing in scope, however, and it sets out elements for designating an item as a defense article even if it is not identified on the USML. An item is a defense article when it:

(1) Is specifically designed, developed, configured, adapted, or modified for a military application, and
(2) Does not have predominant civil applications, and
(3) Does not have performance equivalent (defined by form, fit, and function) to those of an article or service used for civil applications; or
(4) Is specifically designed, developed, configured, adapted, or modified for a military application, and has significant military or intelligence applicability such that control under the ITAR is necessary.[7]

Thus, the analysis whether an item not otherwise listed on the USML is controlled by the ITAR still begins with an analysis of design intent, but the regulation provides conditions that must also be present for the item to constitute a defense article. These conditions—that the item not have predominant civil applications or an equivalent product that has civil applications—are intended to help ensure that only items that are truly military in nature are subjected to ITAR controls.

The USML also extends to any items that are designed specifically for use with another item on the USML. This means that subassemblies or components of defense articles (*e.g.*, an altimeter for an F-16 aircraft) are also ITAR controlled. Under the current system, this often means that even seemingly innocuous items, for instance, fasteners custom-designed for a military aircraft that are similar, but not identical to, common bolts, also may be defense articles.

Technical data is defined as "information . . . required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles."[8] It can include blueprints, drawings, photographs, plans, instructions or documentation. It also includes software directly related to defense articles. It does not, however, include information in the public domain, basic marketing information on function or purpose of the item, or general system descriptions.

As with technical data, the concept of defense services also depends heavily on the definition of defense articles. A defense service is "the furnishing of assistance (including training) to foreign persons, whether in the United States or abroad in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles."[9] But in many respects, the scope of what constitutes a defense service is much broader than what constitutes technical data. This is because, contrary to the definition of "technical data," defense services have no "public domain" exception. Indeed, defense services can be provided using only "public domain" information. For instance, if a US engineer speaks with a foreign engineer about how drag coefficients may be reduced on an unmanned aerial vehicle, even using only public domain information or general principles of physics, this could constitute a defense service.

Understanding which information can appropriately be exchanged over the cloud, therefore, begins with understanding the definition of defense articles and the implications that flow from an item being a defense article. ITAR-controlled software or technical data and defense services are all capable of being transferred in the cloud.

## What Conduct Does the ITAR Control?

The ITAR prohibits exporting goods or technology subject to its control without prior approval from the State Department, absent an applicable exemption.[10] It also prohibits providing defense services to a foreign person without prior approval or an applicable exemption[11] and of potential relevance in cloud computing, the ITAR controls acting as an agent or intermediary on behalf of others in facilitating the transfer of defense articles, which is an activity called "brokering."[12] "Foreign person," "exporting," and brokering are key concepts that are further defined in the ITAR.

### *Foreign Person*

A "foreign person" to whom disclosure or export of articles, data, and services controlled under the ITAR is restricted is defined as any person who is not a US citizen, legal permanent resident (green card holder), or member of a limited set of protected classes (*e.g.*, asylum seeker authorized to work).[13] Foreign persons can be present in the United States on tourist visas, as may be the case with foreign visitors to company facilities (such as on plant tours). Persons present in the United States on work or student visas also are foreign persons under the ITAR.

### *Exporting*

Exporting under the ITAR can occur in several different ways. One is consistent with the ordinary meaning

of the term "exporting:" taking a defense article or technical data out of the United States. The other way in which an export can occur is peculiar to export control laws and is significant in the cloud computing context. An export also occurs when technical data is disclosed to a foreign person. This is called a "deemed export," and it can occur even when the disclosure occurs in the United States. Finally, providing defense services to a foreign person, including in the United States, is an export.[14]

### *Brokering*

A "broker" under the ITAR is someone who "acts as an agent for others in negotiating or arranging contracts, purchases, sales or transfers of defense articles or defense services in return for a fee, commission, or other consideration." The ITAR goes on to provide a non-exhaustive list of activities that constitute brokering, such as "financing, transportation, freight forwarding, or taking of any other action that facilitates the manufacture, export, or import or a defense article or defense service, irrespective of its origin."[15] Brokers must register with DDTC and are subject to licensing and reporting requirements.

## EAR Controls

### What Items Does the EAR Control?

The EAR controls hardware, software, and technology that are civilian in nature or that have both a military and civilian application—dual use. It does not control items that are subject to the ITAR.[16]

Unlike the ITAR, however, which sweeps items within its control using broad categories based on design intent, the EAR relies primarily on a positive list to identify the items controlled. The list that identifies items controlled by the EAR is called the Commerce Control List (CCL). The CCL is divided into 10 categories, numbered 0 through 9, that identify different categories of commodities subject to control. Those categories include nuclear materials and facilities; electronics; lasers and sensors; marine; navigation and avionics; and propulsion systems, space vehicles, and related systems. Of particular relevance to cloud computing, the EAR also controls information technology systems, which includes most encryption technology.[17]

Within each category, the CCL further identifies top-level systems, items, or components; test, inspection, and production equipment; materials; software; and technology subject to control. Depending on the functionality and performance characteristics of a specific commodity, that commodity will be assigned an alphanumeric code, or Export Classification Commodity Number (ECCN), that indicates the level of export controls to which the item is subject. Commodities with features that are viewed as more significant from a US foreign policy or national security standpoint are subjected to more stringent controls. Commodities that are within CCL categories but do not meet the specified functionality or performance characteristics prescribed in an ECCN are designated as "EAR 99."

The EAR also implements United States "Anti-Boycott" laws, which prohibit US firms from yielding to demands from foreign firms to participate in certain foreign boycotts. The most common of these is the Arab boycott of Israel.[18]

### What Conduct Does the EAR Control?

The EAR contains 10 "General Prohibitions."[19] The most basic of these prohibitions, and the one most relevant to the subject matter of this article, is that exports of items controlled under the EAR must occur under a license or applicable exception. In addition, and related to OFAC restrictions discussed further herein, BIS also restricts or prohibits exports to persons who are subject to orders of denial. BIS maintains lists of persons subject to these restrictions that are accessible online, which exporters are expected to check.[20]

As with the ITAR, a foreign national under the EAR is a person who is not a citizen or legal permanent resident of the United States. This includes persons present in the United States on a tourism or work or student visa.[21] An export under the EAR also occurs by sending an item or technical data outside the United States, or by disclosing technical information to a foreign person in the United States.[22]

## US Trade Sanctions

The United States maintains a number of programs that impose trade embargoes and other economic restrictions on dealings with sanctioned entities. These sanctions programs are administered and enforced by OFAC in the Treasury Department.

In general, there are two types of OFAC sanctions programs: (1) "country-based" and (2) "list-based." Country-based programs prohibit virtually all transactions with persons or entities in the sanctioned country. List-based programs prohibit dealings with specified individuals, classes of individuals, and/or organizations and their representatives.

Country based programs include Burma, Cuba, Iran, North Korea, Sudan, and Syria. List-based sanctions programs include the Balkans, Belarus, Democratic Republic of Congo, Iraq, Ivory Coast, Lebanon, Liberia, Narcotics Trafficking, Non-Proliferation, Somalia,

Terrorist Organizations, and Zimbabwe. Entities and individuals that are subject to trade sanctions are identified on the Specially Designated Nationals list, which is available online.[23]

Under either type of sanctions program, the types of transactions that are prohibited, as well as the circumstances under which certain transactions may take place, vary by program and are set out in the executive orders and regulations establishing and implementing the programs.

Sanctions programs may impact the activities of cloud users and providers in a number of respects. They may severely limit or prohibit entirely the exportation of any goods (including software and technology) from the United States to the embargoed country or entity. They may prohibit or restrict the ability to provide services in sanctioned countries or to sanctioned entities. In addition, while sanctions programs apply in general to US persons and entities, wherever located, it is generally unlawful for US persons to facilitate or assist another person—even one to whom OFAC sanctions do not apply. This "facilitation" prohibition can arise where, for instance, a foreign affiliate of a US company desires assistance from the US company or its employees in performing work in an embargoed country. OFAC regulations can severely restrict or prohibit the US entity from providing such assistance.

The impact of sanctions programs on cloud computing can be particularly significant because, unlike export controls, sanctions are largely content neutral. They prohibit most interactions with sanctioned persons, entities or countries, irrespective of the substance of the technology or services being provided.

# Penalties

The penalties for violating ITAR, EAR, or OFAC restrictions can be severe. When violations are intentional and willful, companies and individuals can be subject to criminal sanctions. Individuals can be subjected to imprisonment of up to 20 years, and individuals and corporations can be fined up to $1,000,000 per violation.

Violations that are not willful can still be punished by civil and administrative penalties of up to $250,000 for violations of the EAR and OFAC and $500,000 for violations of the ITAR. In addition to monetary penalties, individuals and companies can be excluded from exporting or from government contracting.[24]

The risks to cloud users and cloud providers for noncompliance with US trade control laws are significant. To avoid trouble, it is important to understand both what the law requires and the ways in which the cloud can implicate US trade control laws.

# US Trade Control-Related Risks for Cloud Users and Providers

While cloud computing services and technologies simplify sharing of information and services, this ease with which information can be shared presents enhanced compliance risks against the backdrop of the US laws and regulations that are intended to restrict the sharing of information. In substance, US trade control laws do not differentiate between sharing information over the cloud and sharing it in person, in hard copy, or over traditional email. However, the degree to which the cloud facilitates sharing and distribution of information and the extent to which data can become distributed in the cloud present novel challenges in complying with those controls.

## Agencies Speak on Cloud Computing

Regulatory agencies have issued limited guidance on trade controls as they relate to cloud computing. In 2009, BIS issued the first of two advisory opinions on cloud computing.[25] The opinion addressed whether and to what extent the EAR applied to cloud computing. BIS concluded that providing computational capacity through cloud computing, without more, is not "subject to the EAR." In brief, this means, from BIS's perspective in any event, that computational services can be provided via the cloud without regard to the nationality or location of the recipient, provided that no other export of controlled software or services occurs in connection therewith.[26] BIS thereby expressly relieved providers of computational capacity via the cloud of the obligation, in most cases, to inquire as to the nationality of their users. At the same time, transferring via the cloud software that is subject to the EAR would constitute an export. The 2009 opinion held, however, that cloud computing providers generally are not exporters of data stored by users on their systems.

In 2011, BIS provided additional guidance on cloud computing.[27] The 2011 opinion responded to a question whether a cloud provider needed to obtain deemed export licenses for foreign national IT administrators who service and maintain their cloud computing systems. Under the facts presented in the opinion, those IT administrators may obtain incidental access to export controlled information in connection with performing their work.

That opinion held, through somewhat convoluted logic, that a cloud provider would not be performing a deemed export when a foreign national employee of the cloud provider viewed export-controlled information incidental to the performance of his or her work for the provider. Therefore, on the facts presented in the request for the

opinion, the cloud provider did not need to obtain deemed export licenses.

In March 2012, OFAC provided guidance on its licensing policy concerning exports to Iran of software and services incidental to personal communications.[28] In order to permit the free flow of information to Iran's citizens, OFAC's Iran sanctions permit the export of "services incident to the exchange of personal communications over the Internet," including instant messaging, email, and social networking, provided these are free of cost to the user. OFAC's March 2012 guidance clarified that this general license permits the export to Iran, free of charge, of software and services that permit and facilitate personal communications. OFAC provided as examples messaging clients, non-fee based Skype, Web browsers, document readers, personal cloud storage, and such. This guidance also indicated that OFAC may issue specific licenses on a case-by-case basis of fee-based software and services, provided that they perform a function similar to those free applications identified in the guidance. Examples of fee-based software and services that OFAC indicated it may issue specific licenses to export to Iran include Web hosting, Skype Credit and Google Talk, fee-based mobile apps, and online advertising.

## Issues for Cloud Users

Although the guidance issued by BIS and OFAC leaves many questions unanswered, it helps complete a picture of how US trade controls apply to cloud computing. One basic point that emerges is that users, not providers, must be responsible for the content they place in the cloud. When an engineer wishes to share technical data with a colleague in India, for example, the engineer must know whether and how the information is controlled and what measures are necessary in order to share the information. Failure to appreciate the limitations on disclosing information via cloud computing—in the same way as trade controls apply to information exchanged via more traditional methods—can lead to violations.

More complicated questions arise with regard to the compliance risks and challenges facing institutional users of the cloud. Again, it generally is the user's obligation to comply with trade controls with regard to its own data. This applies whether the user is an individual or an enterprise. When businesses migrate to the cloud, therefore, it is important that the enterprise user exercise due caution to help ensure that data will not be placed in the cloud or, once placed in the cloud, handled in a manner that gives rise to potential export violations by the user.

As an initial step of trade compliance, companies must be aware of the proper export jurisdiction and classification of all goods and technology within the company. This is critical to a company's ability to exercise the appropriate controls over those goods or technology. But when migrating enterprise data infrastructure to the cloud, companies may surrender a significant degree of control over their data even when it is simply being maintained within the company's own IT systems. An important initial question to mitigate risks from migrating to the cloud is where the servers, and hence the data, will be located. Under the ITAR and the EAR, technical data may be exported by being taken out of the United States.[29] If controlled technical data is stored on a server located outside the United States, there is a strong argument that an export of the data has occurred. This can occur even without knowledge or intent on the user's part.

Even when servers are physically located within the United States, there remains the issue of potential deemed exports occurring when foreign national employees of cloud providers have access to controlled information. BIS's 2011 advisory opinion stated that cloud providers do not make a deemed export when a foreign national employee gains incidental access to data maintained by the cloud provider. BIS did not state that a deemed export does not occur in this circumstance. Nor did it state that the cloud user that placed the data in the cloud is not responsible for a deemed export. Indeed, a strong argument could be made that the cloud user is responsible for the deemed export.

Cloud users must therefore be as vigilant as ever with regard to knowing which export controls apply and guarding against unauthorized exports, including deemed exports. The nature of the cloud complicates this compliance challenge. Cloud users should conduct due diligence on cloud providers both to determine the geographic location of their servers and the nationality of their employees. Several cloud providers offer "ITAR-compliant" cloud services that, presumably, seek to address these concerns. Where such options are not available, however, potential users of cloud computing services may face challenges in taking steps to assure reasonable compliance.

## Issues for Cloud Providers

The BIS and OFAC guidance limit the circumstances in which cloud providers may be subjected to liability for export violations arising from content placed on their servers by users. They do not, however, mean that cloud providers are shielded from liability under US trade control laws. First, DDTC has yet to issue guidance on its own interpretation of the application of ITAR controls to cloud computing, which could be at variance with the guidance already issued by BIS. Furthermore, the 2011 opinion regarding deemed exports was expressly limited to the facts presented, in which the foreign national employee in question was accessing data as an incidental part of doing his job for the provider.

There is nothing in the advisory opinion to suggest that the outcome would be the same if the foreign national accessed the data deliberately or in a manner other than incidental to the employee's performance of his job. Indeed, prudence may warrant that a cloud provider seek to be placed on notice when users place export controlled information on its servers and take steps to prevent access by employees beyond what is necessary to perform their jobs.

The ITAR's restrictions on brokering present interesting, even if unresolved, questions concerning whether and in what circumstances a cloud provider can be considered to be acting as a "broker." The limits of the ITAR's definition of brokering is a subject of much debate, but at the core of that expansive and amorphous definition is activity involving arranging a sale of a defense article or defense service on behalf of others. Because of the intermediary nature of cloud services, to the extent that cloud providers may provide services that have the effect of assisting a sale relating to a defense article, there is an argument that the cloud provider is engaging in brokering. Cloud providers must be aware of this possibility and analyze their risks accordingly.

Trade sanctions present thornier issues for cloud providers. As discussed above, in the case of Iran, OFAC has authorized via general license the export of software and services that facilitate personal communications, and has indicated a willingness to issue specific licenses for fee-based software and services that serve the same function. But, in many cases, this would not apply to cloud providers' services for commercial communications.

The possibility that US cloud providers may be presented with business opportunities that could implicate sanctions programs is not remote. Many countries do not maintain trade embargoes that are as restrictive as those imposed by OFAC. It is not uncommon for EU companies (as an example) to transact business in countries subject to comprehensive US sanctions. US-based cloud providers must take care not to provide technology or services to sanctions targets.

Assume that a European company located in the European Union, which is not bound by US sanctions programs, seeks a cloud computing provider to support its global operations. Those operations include offices and personnel in Iran. The cloud provider will need to provide both cloud services themselves as well as technical support as needed to all employees of the EU- based company.

Because this business arrangement could give rise to a US company or its employees providing services to persons and companies in Iran, there is a significant potential for OFAC violations. Such potential violations could occur irrespective of the substantive information being exchanged. When undertaking international business opportunities, cloud providers must be sensitive to the risk of sanctions violations, with an eye toward the global reach of their clients' operations.

But OFAC regulations do not only prohibit many interactions between US persons and companies and sanctioned entities. They also prohibit most acts that would help or enable a non-US person to perform the act from which the US person is prohibited. OFAC's rules regarding "facilitation" can make managing sanctions risks particularly challenging. Those rules are so broad that any involvement by a US person or company in effecting a transaction involving a sanctioned country or entity must be carefully scrutinized. Referring opportunities to foreign affiliates, may implicate OFAC sanctions regulations.[30] There also are provisions that limit restructuring one's own business in order to permit work with sanctioned entities to occur.[31] Cloud providers must therefore be cautious not only with respect to identifying business opportunities that may implicate US trade sanctions, but also with regard to how they proceed when problematic opportunities are identified.

# Conclusion

US trade controls place important restrictions on both using and providing cloud computing services. Those controls are pervasive and can be complex, and the consequences of violating them can be severe for both individuals and corporations. While regulatory agencies have provided some guidance on the subject to date, it is limited and leaves many questions unanswered. It is therefore critically important for cloud users and providers to take a considered approach to understanding the relevant controls and how they may apply in the cloud computing context.

1. Over the years, there have been various efforts to unite these two control regimes or otherwise modify the manner in which jurisdiction is divided between them. While significant progress toward this goal has been made in recent years, as of this writing, the system is as it has been for decades.
2. 22 C.F.R. Parts 120-130.
3. 15 C.F.R. Parts 730-780.
4. *See generally* 31 C.F.R. Parts 501-598.
5. 22 C.F.R. § 121.1; *see also* 22 C.F.R. § 120.6; 22 C.F.R. § 120.3.
6. For instance, the USML does not identify specific aircraft that are subject to ITAR, but rather states that ITAR controls aircraft "specifically designed, modified or equipped for military purposes." 22 C.F.R. § 121.1, Category VIII(a). At the same time, the USML specifies the body armor subject to ITAR controls not with regard to its design intent, but rather with reference to performance characteristics. 22 C.F.R. § 121.1, Category X(f) (removing from control under Category X body armor that is classified as Types I through III-A according to National Institute of Justice classifications).
7. 22 C.F.R. § 121.3.
8. 22 C.F.R. § 120.10.
9. 22 C.F.R. § 120.9.
10. 22 C.F.R. § 123.1; 22 C.F.R. § 125.1.

11. 22 C.F.R. § 124.1.
12. 22 C.F.R. Part 129.
13. 22 C.F.R. §§ 120.15–120.16.
14. 22 CFR § 120.17.
15. 22 C.F.R. § 129.2.
16. 15 C.F.R. § 734.3.
17. 15 C.F.R. Part 774, Supp. 1 Category 5, Part 2.
18. *See* 15 CFR Part 760.
19. 15 CFR § 736.2.
20. These lists include the denied persons list, the entity list, and the specially designated nationals list, among others. *See http://www.bis.doc.gov/complianceandenforcement/liststocheck.htm.*
21. 15 C.F.R. § 734.2(b).
22. *Id.*
23. *http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx.*
24. 15 C.F.R. § 764.3 (EAR); 15 U.S.C. § 1705 (EAR and OFAC); 22 U.S.C. § 2778 (ITAR).
25. *http://www.bis.doc.gov/policiesandregulations/advisoryopinions/jan13_2009_ao_on_cloud_grid_computing.pdf.*
26. "Subject to the EAR" refers essentially to all commodities within the United States or of US origin that are not otherwise controlled under ITAR, OFAC, or Nuclear Regulatory Commission or Department of Energy regulations. Certain informational materials and public domain software also are not "subject to the EAR." Even when a commodity is not subjected to licensing controls by the Commerce Control List, it may be "subject to the EAR." As a practical matter, this means that the commodity is still subject to certain of the non-licensing related restrictions of the EAR, such as the prohibition on exporting to denied persons. *See* 15 C.F.R. § 734.3.
27. *http://www.bis.doc.gov/policiesandregulations/advisoryopinions/jan11_2011.pdf.*
28. *http://www.treasury.gov/resource-center/sanctions/Programs/Documents/internet_freedom.pdf.*
29. *See supra*, notes 14 and 21.
30. *See*, *e.g.*, 31 C.F.R. § 560.208.
31. *See*, *e.g.*, 31 C.F.R § 560.417.

Copyright © 2012 CCH Incorporated. All Rights Reserved.
Reprinted from *IP Litigator,* September/October 2012, Volume 18, Number 5, pages 24-30,
with permission from Aspen Publishers, Wolters Kluwer Law & Business, New York, NY,
1-800-638-8437, www.aspenpublishers.com