# YEAR END REVIEW OF EXPORT CONTROL ISSUES

**by**

**Raymond F. Sullivan, Jr.**

***Shareholder***

**BAKER DONELSON BEARMAN CALDWELL & BERKOWITZ, PC**
**555 Eleventh Street NW**
**Washington D.C. 20004**
**Phone: 202-508-3466**
**Fax: 202-220-2266**
**Email: rsullivan@bakerdonelson.com**

# YEAR END REVIEW OF EXPORT CONTROL REGULATORY CHANGES AND PROPOSED CHANGES

A number of recent changes and proposed changes in the export control regulatory scheme have occurred recently. We have prepared an extensive summary of these recent developments, as year-end approaches, which is available at your request. Below is a brief outline of the areas where these changes and proposed changes have taken place. If you would like additional information on these specific areas; or, would like to receive a copy of the full summary please let us know.

# YEAR END REVIEW OF EXPORT CONTROL ISSUES

## 1. Dual-Use Export Control Developments

**1.1 Proposed License Exception ICT for Intra-company Transfers**. The Bureau of Industry and Security (BIS) issued a **proposed amendment to the Export Administration Regulations (EAR)** to create a new License Exception ICT for companies to export, re-export, or transport (in-country) dual-use products such as software and technologies to and among their "wholly-owned or controlled-in-fact" non-U.S. entities and foreign national employees. *73 Fed. Reg. 57554* (October 3, 2008). Industry has long sought a broad, unfettered License Exception like ENC for intra-company transfer of encryption source code and technology for use and product development. However, in the view of most exporters, the form of the proposed rule that resulted from interagency review is very cumbersome and a License Exemption in name only.

To the extent that License Exception ICT applies, companies no longer need to obtain and maintain a multitude of individual licenses to meet the requirements of day-to-day intra-company transfers, including deemed exports to employees. This approach removes the burden of applying for, tracking and reporting on a number of single licenses and results in a streamlined exporting process for both those that successfully meet the ICT requirements and BIS. The proposed rule arises from years of proposals from many exporters and trade associations (including the Deemed Export Advisory Committee) that U.S.-based companies and those based in many allied nations should be considered trusted entities to handle exports among affiliates and employees without the need for licenses. Many companies today apply for more deemed and other intra-company export licenses to "talk to themselves" than they do to export to customers since their research and development technologies and source code are more likely to require licenses than end-products.

However, many will likely think that the burdens of applying for, obtaining, and maintaining the criteria to establish themselves as trusted enough for License Exception ICT will outweigh the benefits in its proposed form. This is more like the old Distribute License or Special Comprehensive License or Validated End-User (VEU) (or a security clearance) than any License Exception and seems to require that a company prove its innocence in its application, annual reports and audits rather than being considered a trusted end-user.

First, a company must apply for authorization to use License Exception ICT, a requirement only associated with License Exception ENC for products. The **"parent"** company applicant must be incorporated or have its principal place of business in a

country listed in proposed new Settlement No. 4 to EAR Part 740.[1] The application must provide details on the applicant and each eligible wholly-owned or controlled-in-fact **"user"** and **"recipient,"** which can be in any country except Country Group E or North Korea. The intended difference, if any, between a "user" and a "recipient" is not clear. Presumably, some users and recipients may not be approved.

Experts will need to **list Export Control Classification Numbers (ECCN) to be covered** and likely negotiate their application with BIS and other reviewing agencies. Note that exports that would not qualify for License Exception under EAR 740.2, including Missile Technology controlled and certain "space qualified" items (ECCN5 3A001.b.8, 3D001, 3E001, 6A002.e, 6A008.j.1, 6A998.b, 6D001, 6D002, 6D991, 6E001, 6E002, 6E101, 6E99l), ECCNs 2A983, 2D983, or 2E983, or QRS-1 1 Micro-machined angular rate sensors, could not be exported under License Exception ICT. Significant Items-controlled ECCNs also cannot be exported under ICT. License Exception APR cannot be used to authorize re-exports that otherwise would be authorized, which is not the case for licensed exports. Also, encryption items controlled under ECCNs 5X002 cannot be exported and re-exported under ICT, mainly because License Exception ENC permits the vast majority of such exports with far fewer restrictions (exception for companies headquartered in Argentina or South Korea). Finally, the preamble reminds exporters that foreign direct products of U.S. origin technology or software may be subject to license requirements under General Prohibition 3. (We have extensive guidance on that subject for those clients who desire more information. It rarely applies anymore, but clients should approach application with caution. Regulators have discussed making the Prohibition more restrictive).

Items exported may be only for **internal use.** Any re-export or retransfer must be authorized by another License Exception (other than APR), NLR, or a license.

Companies need to create and include in their application an extensive **internal control plan** covering technology and other applicable exports to even be considered for the exception. Each affiliate "user" of ICT must adopt the compliance plan. The plan described in EAR proposed 740.19(d) consists of nine parts, including a corporate commitment to export compliance, a physical security plan, information security plan, personnel screening procedures, training and awareness program, self-evaluation program, letter of assurance for software and technology, employee signing of non-disclosure agreements addressing export controls, and a review of end-user lists. The

[1] Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, German, Greece, Hungary, Iceland, Ireland, Italy, Japan, South Korea, Latvia, Lithuania, Luxembourg, Malta, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States. (This is the same list as Supp. 3 for License Exception ENC, with the addition of Argentina and South Korea. Let's recommend adding them to Supp. 3 and just have one list.

complexity of such plans varies with the types of products exported, where they are exported and the type of end user. Evidence of implementation of the screening, training, and self evaluation elements of the plan must be submitted. BIS may require vision of the plan before authorizing the use of ICT. Many exporters have comprehensive export compliance programs that will meet most of these criteria, but the depth of the criteria for License Exception ICT goes beyond standard Export Management systems. For example, the proposed rule says that any deficiencies uncovered in self evaluations must be voluntarily disclosed; otherwise, the ICT authorization could be revoked.

The **application review process** is the same as for an export license, involving other agencies and the normal dispute resolution procedures. The agencies will consider prior licensing history to determine whether they believe ICT is needed, including the requested ECCNs (which obviously will change with a dynamic company), and will also consider prior violations and other negative issues in deciding whether and to what extent to approve the plan.

Once License Exception ICT authorization is approved, companies are not in the clear. **Annual reports** must be submitted to BIS. The reports must include a detailed list of all foreign national employees, including name and birth dates (which will likely cause problems under EU and other privacy laws), and who received what items (including technologies or source codes) under ICT. Companies must also submit new entity information and changes in information submitted before continuing to use ICT for such entities.

Many companies are now running **cost benefit analyses** to figure out the detriment this annual reporting alone will cause compared to the existing process. The final verdict is still unknown due to the vague descriptiveness of the rule pertaining to this list. If, for instance, a company must list all previous recipients of technology and source code prior to receiving the license in the first place, as well as identify the specific technologies received by specific foreign nationals in the annual reports, the costs could far outweigh the benefits.

In addition to this rigorous requirement, companies must undergo an **audit by BIS biannually** if there are any reasons suggest wrongdoing. In this scenario the audit is a BIS initiative. The outcome of such audits will be interesting. As the proposed rule stands, there are very few clear lines to determine what is acceptable to meet ICT internal control program standards and what is not. Those who operated with the old Distribution License recall that inexperienced auditors sometimes substituted their own judgment for what types of procedures were acceptable. One auditor might suspend a company whereas another might not. Most government auditors are experienced and reasonable. Nevertheless, this is a heavier burden to impose on exports among supposedly trusted parties than what is currently imposed on most licensed exports to third parties.

**BIS** performed its own **cost-benefit analysis** and determined that approximately 200 companies applied for licenses that fell under the umbrella of ICT. Of these companies, BIS determined that only 17 would benefit from License Exception ICT. The

majority of these companies, in the eyes of the BIS, have already established and implemented strong internal control programs. Only two companies without internal control programs in place surpassed the cost benefit threshold. The cost of constructing an internal control program that meets these standards, for most companies, is more expensive and time consuming than simply applying for licenses. Therefore, the amount of time and effort to pass the proposed rule appears to exceed the gains that only a handful of companies would reap.

**1.2 BIS Issues "Encryption Simplification" Regulation; Encryption Regulations Remain Extraordinarily Complicated.** As part of its implementation of Presidential National Security Directive *55* issued in January 2008, BIS has published its latest interim final rule revising the EAR's encryption provisions. *73 Fed. Reg. 57495* (Oct. 3, 2008). It partially delivers on its title of "Encryption Simplification" by eliminating a few regulatory requirements (notifications for weak crypto, KMI and technical assistance), adding some new exceptions from review (most promising for "ancillary cryptography" in products while less useful for "personal area networks"), and to some degree, cleaning up the extremely convoluted encryption regulations. These changes notwithstanding, the encryption provisions, remain the most complicated parts of the EAR. Indeed, these changes required 18 pages of fine print amendments to no less than seventeen EAR sub-parts (the changes eliminated only two sub-parts), three part supplements, and six ECCNs. **Please let us know if you would like a copy of our updated Power Point explanation of post-simplification encryption controls.**

**1.2.1 This Rule is Not the Fundamental Encryption Reform Sought by Exporters ; That Will Take More Time. Encryption controls** take up some 20 percent of BIS' time, and apply to more and more products as the industry has incorporated commonly available encryption functionality into most software, computer and telecommunications hardware, and microprocessors. Note 1 to Commerce Control List Category *5*, Part 2 states that products with even minor encryption functionality are treated as encryption products. (This reverses the normal *Interpretation* 12 to EAR 770.2(b) that a component loses its ECCN when incorporated into something else.) Increasingly burdened by complex product classification and reporting requirements, the industry has been pushing for more fundamental encryption reform, favoring structural simplification of the current complicated system of encryption export controls, harmonizing U.S. interpretations with those of our Wassenaar partners, and eliminating certain burdensome unilateral controls and requirements for mass market encryption items.

The inclusion of encryption reform in Presidential National Security Directive *55* stimulated more high-level attention to the issue, but the rule does nothing to implement most of the essential recommended reforms. Assistant Secretary for Export Administration Chris Wall acknowledged as much in his speech at Update 2008 when addressing this regulation.

These are not fundamental reforms, but they are a start. Still to be addressed are issues related to open cryptographic interface requirements, reporting of exports under

License Exception ENC, national security controls on TSU-eligible encryption source code, and controls on chips and other encryption components and technology for mass market products. A more comprehensive approach to encryption simplification will take time, but we are already beginning that process.

On balance, the changes are underwhelming, and unlikely to have significant impact on compliance with U.S. encryption export controls, with the possible exception of the concept of self-classifiable items with only "ancillary encryption." The existing system of prior review and classification remains otherwise essentially undisturbed, with the changes removing or relaxing requirements on encryption items that, at least in terms of what we see in our practice, represent old technology and only a small section of encryption items. Most of the changes consist of tinkering with parameters, adding limited exclusions from prior review requirements, recasting prohibitions on export of technical assistance as prohibitions on technical data export controls, and attempting to streamline regulatory language to eliminate confusing or outdated provisions.

**1.2.2 Elimination of 5A992/5D992/ Weak Cryptography Notification Requirements.** The rule eliminates the requirement for prior e-mail notification to self classify 5A992/5D992/5E992 "weak" encryption items (56-bit or less symmetric, 512-bit asymmetric or less, and 112-bit or less elliptic curve cryptographic items) prior to export, and likewise eliminates notification requirement for 5X992 self classification of mass market items with no more than 64-bit symmetric crypto. In light of the standardization of 128 bit or stronger symmetric encryption algorithms as a baseline industry standard, following adoption of U.S. Government Federal Information Protection Standards 197 (FIPS 197) in 2001, it is unlikely these relaxations will affect a large number of encryption products. It has been rare for Baker Donelson to assist a client with only a weak crypto item e-mail notification, although the provision is sometimes useful to get a new product to market before an encryption review on a stronger version can be completed.

**1.2.3 Elimination of EAR Part 744.9 Technical Assistance Prohibitions.** The rule also eliminates EAR Part 744.9, which imposed a license requirement on "U.S. persons" providing "technical assistance" to aid a foreign person in the development or manufacture outside the United States of 5A002 or 5D002 equivalent foreign encryption commodities and software (other than publicly available TSU eligible items). This provision was a leftover from the grafting of ITAR controls on encryption onto the EAR when jurisdiction was transferred in 1996, as it mirrors the concept of controlling an export of an ITAR defense service even when all technology was decontrolled public domain technology.

Eliminating this trap for the unwary is somewhat helpful in simplifying the structure of the encryption controls, because it was something of an outlier, residing as it did amongst the various proliferation-related controls in Part 744, and because it imposed controls on activities of "U.S. persons" regardless of export, an unusual basis for control under the EAR. The EAR primarily applies to actions involving goods, technology and

software that are subject to the EAR, not to the actions of people (NB., Part 744.6 does contain counter-proliferation based licensing requirements applicable to the activities of U.S. persons that do not involve exports). Fortunately, OEE has not enforced this provision to our knowledge, but it was difficult to advise procurement officials as to whether discussing with non-U.S. suppliers how to revise their products to meet security requirements might or might not be subject to this control.

However, it is not a major relaxation in license requirements, since removal of this provision was coupled with a warning in the License Requirements notes to ECCN 5E002, that BIS considers the provision of technical assistance that incorporates or draws upon U.S.-origin encryption technology to inherently involve the release of 5E002 technology, which would trigger licensing requirements if the technology is exported. (That is not the case for publicly available technology, which the warning does not mention.) These 5E002-based restrictions on the export of U.S.-origin encryption technology already existed, and BIS claims to have removed the 744.9 provisions because they essentially overlapped with these technology export controls. The Federal Register notice points out that the industry recognized this and were simply adding Part 744.9 authorization requests as "ride-alongs" to 5E002 technology export licenses.

**1.2.4 License Exception ENC 740.17 Changes, Including "Ancillary."** EAR 740.17, License Exception ENC, has been reorganized, but with only few substantive changes. License Exception ENC remains available to authorize exports without a license of 5A002, 5D002 and 5E002 items to destinations other than the five current embargoed countries (Cuba, Iran, North Korea, Sudan and Syria, also known as the "T-5"). The rule retained the basic format, which permits use of License Exception ENC without submission of a encryption review request in some circumstances involving transfers to U.S. subsidiaries or companies headquartered in the License Free Zone (LFZ), but requires the submission of an encryption review request prior to export for general distribution to third parties in most cases, which a 30-day waiting period imposed while the review request is pending for destinations outside the LFZ. Restructuring of the language and edits to provisions of subpart (a) and (b)( 1) to be clearer to the first time reader, will likely confuse those who are familiar with the structure of the last eight years. Except for substantive changes discussed below, these rewrites do not do much.

Supplement No. 3 to Part 740 of the EAR now has a more descriptive title: "License Exception ENC Favorable Treatment Countries." BIS also added Bulgaria, Iceland, Romania and Turkey (recently admitted RU and NATO countries), as well as Canada (which is generally an NLR destination for encryption items), expanding the total number of countries on the list to 35. This list had been informally called the "License Free Zone" or "LFZ" by many practitioners.

Provisions retained include the 740.1 7(b)(2) and (b)(3) structures for ENC-R and ENC-U classified products given that thousands of existing CCATS classifications cites those provisions. The new regulations officially adopt the informal terminology that has been used by both BIS and the industry since the 2004 encryption regulation changes

"ENC Unrestricted" versus those that cannot be exported under y740. 1 7(b)(2) to "government" end-users outside the LFZ as "ENC Restricted." The formal references to these provisions required citation to these particular sub-sections, which was not a major problem, other than adding to the need for exporters not conversant with chapter and verse of the regulations (and even some experts) to have to crack the regulations to make sure they were citing the correct provision. BIS seems to have realized that these terms have become the *de facto* terminology and has incorporated them into the regulations.

**1.2.4.1 New Exemptions from Prior ENC Review Requirements for "Ancillary Crypto" and "Personal Area Networks."** **A** new provision permits ENC exports and re-exports of 5A002/5D002 commodities and software using cryptography up to 80 bit symmetric, 1023 asymmetric, or 160 bit elliptic curve algorithms under ENC to government and non-government end-users worldwide (except for the embargoed countries) immediately upon registration of an encryption review request. See EAR 740.17(b)(1)(ii). (5A002, 6D002, and SF00: items with stronger encryption can still be exported under ENC to the LFZ immediately upon registration of an encryption review request.) Our understanding is that these limits were raised to relax controls on the use of the 64-bit CAST algorithm in non-mass market items, as well as certain 80-bit algorithms commonly used in GSM telecommunications devices. These limits may also foreshadow U.S. proposals to decontrol 80 bit symmetric or less encryption algorithms from 5X002 controls at the multi-lateral Wassenaar meeting in December. (Note: The existing reporting exemption for 64-bit symmetric or less SA/D002 products was not raised to mirror the new 80-bit symmetric level. While these items can be shipped worldwide immediately upon registration, they may still be subject to semi-annual reporting requirements.) BIS admits that this change will affect very few products, but could not persuade NSA to raise the effective decontrol limits to 128, 2048 and similar.

The most significant change in the rule was to eliminate mandatory encryption review prior to using ENC for items performing only "**ancillary cryptography,"** defined as:

> The incorporation or application of "cryptography" by items that are not primarily useful for computing (including the operation of “digital computers”) communications, networking (includes operation, administration, management and provisioning) or information security.

**N.B.** Commodities and software that perform "ancillary cryptography" *(i.e.* are specially designed and limited to: piracy and theft prevention for software, music, etc. games and gaming; household utilities and appliances; printing, reproduction, imaging and video recording or playback [but not videoconferencing]; business process modeling and automation [*e.g.*, supply chain management, inventory, scheduling and delivery]; industrial manufacturing or mechanical systems [including robotics, or factory or heavy equipment, facilities systems controllers including fire alarms and HVAC]; automotive, aviation and other transportation systems). Commodities and software included in this

description are not limited to wireless communication and are not limited by range or key length.

The exception provides meaningful relief for the items in the above examples, but exporters should note that these are examples and are not limiting. We have obtained a classification for e-commerce software as ancillary and expert to be able to fit other items in this definition, but we will likely be discussing them with BIS experts for awhile to see if they agree with our interpretation of what items are covered by this fairly subjective term. Note that many of these items may already be eligible for either self-classification as 5A992 items due to the type of cryptography use (*e.g.*, limited to password encryption or authentication, decryption lonely of copy protected software) or for the already existing exemptions from prior review requests for items using only short-range wireless encryption components, but even then, it may help provide a clear path when existing decontrol notes have not kept pace with technology changes.

The Rule also added an exemption from the requirement to file encryption review requests for wireless "**personal area network"** items that implement only published or commercial cryptographic standards (IEEE 802.15.1, class 2 & 3 but not class 1 [100 meter]) and where the cryptographic capability is limited to a nominal operating range not exceeding 30 meters according to the manufacturer's specifications. This could provide some relief for manufacturers of wireless telephone and data devices, but most think that all such products would have been already be eligible for the existing exemption for short-range wireless products (802.15 and 802.1 class 1). Again, this may foreshadow a U.S. Wassenaar decontrol proposal.

**1.2.4.2 Non-U.S. Encryption Products**. The ENC revisions also modified EAR 740.17(b)(4) to state that foreign-produced products that are developed with or incorporate U.S.-origin encryption source codes, components or toolkits are exempt from prior review requirements, provided that the U.S.-origin items have been appropriately reviewed by BIS and cryptographic functionality has not been changed. That section was amended to add a sentence stating that such foreign items include those "designed to operate with U.S. products through a cryptographic interface." This statement clarifies that such items are exempt from review requirements, but at the same time implies that such items are in fact subject to U.S. jurisdiction without more. However, we do not think that BIS can amend the EAR to expand extraterritorial jurisdiction beyond what is set out in EAR 734.3 and 736 *(i.e.*, there needs to be some U.S.-origin content or be the direct product of U.S.-origin NS controlled technology for the non-U.S. origin items to be subject to the EAR). This deserves a comment in the form of a statement, not a question.

This change reflects an increasingly conservative interpretation by BIS in recent years of the applicability of ENC review requirements to items that do not themselves incorporate encryption functions algorithms in their codes, but rather call out to separate products with encryption functions or to operating system elements via a cryptographic interface *(e.g.*, the Microsoft Crypto API) to provide security functions. Such items have been informally dubbed "crypto-aware" items by the industry and BIS and are controlled

as products designed or modified to use cryptography (see ECCN 5D002). This is usually a shock to programmers new to encryption controls. Whether such items are subject to prior classification requirements has been a hotly debated question over the years, with reasonable arguments made on both sides. As a result of these discussions, BIS had agreed to accept e-mail notification of a general description items calling on the MS CAPI plus Part 742, Supplement 6 information as sufficient to permit the items to be derivatively classified under the same ECCN as the item it calls on, provided that item being called upon had been previously reviewed by BIS *(e.g.*, Windows, Java mass market programs). These were informal interpretations, though provided in public meetings. So, for example, if an item called on Windows XP through the Microsoft Cryptographic API, and had no other controlled crypto functions, it would be 5D992 after notification. Current BIS personnel have changed this interpretation in recent statements at conferences, as well as to us in the context of classification reviews, where they have said that a "crypto-aware" product cannot be derivatively classified based on the classification of the items call upon, bur rather should be classified as new encryption items via the ENC review procedure. This may be a reasonable interpretation, but it nonetheless represents a rollback of prior interpretations that were also reasonable and have been relied upon in the past. Applying this new, more expansive interpretation is much less defensible for foreign products that have no U.S. content, and thus are not subject to the EAR.

Section 740.17(c) clarifies that non-U.S.-origin products incorporating ENC exported products are subject to the same ENC-R or other applicable restrictions as they did undergo review under the EAR.

**1.2.4.3 Changes to ENC Restricted Parameters.** The Rule slightly relaxed most control parameters for ENC-Restricted items but probably with little practical effect. For example, the data throughput parameters for ENC-Restricted WAN/MAN/VPN equipment was raised from 44 Mbps to 90 Mbps for wireless and 154 Mbps for wired equipment, but there are few items in that space. (BIS even admitted in the *Federal Register* that this change will likely have no practical effect, but reflects an attempt towards catching up part of the way to the performance levels of high-end routing equipment.) The parameters for other items covered by ENC-Restricted were increased as well, so exporters with ENC-Restricted equipment should review carefully to determine if their products are released by the changes, and if so, submit an updated encryption review to confirm ENC-Unrestricted eligibility.

**1.2.4.4 ENC Reporting.** The primary burden of being subject to 5D002 ENC controls (instead of 5D992 Mass Market) is the semi-annual reporting requirements. There were already a number of exemptions to the reporting requirements. The Rule added an exemption for items that do not need prior review for ENC classification (including **"ancillary crypto"** and **"personal area networking"** items), and also added a paragraph indicating that **BIS can grant waivers** of reporting requirements on a case-by-case basis. In some cases, we were able to secure *ad hoc* reporting exemptions from BIS for ENC-Unrestricted items, so this revision is a very welcome formalization of that

process. No criteria are provided, but we have had success with products that almost qualify as mass market and products where all encryption was internal and not available to the user. As mentioned above, the existing exemption from reporting for 64 bit symmetric 5D002 items was not raised to 80 bit symmetrical to exempt from reporting some items that are now eligible for worldwide distribution upon filing of a classification review request.

**1.2.5 5A992/5D9921 742.15 Mass Market and Other Decontrol Changes.** The rule reorganized ECCNs 5A992 and 5D992 to differentiate between items that qualify as 5D992 based on having weak cryptography (*e.g.,* 56 bit symmetric or less) and/or limited encryption functions (*e.g.,* authentication/password only) versus "strong" crypto items that are decontrolled from 5A002 or 5D002 as Mass Market items following review and classification by BIS. This was done by reorganizing the paragraphs of the two ECCNs and eliminating the sub-paragraphs since there is currently no difference between AT1 and AT2 controls. So exporters with existing 5A992 and 5D992 classifications should review the regulation to confirm the correct paragraph number that applies. The new Mass Market sub-category is now found at 5D92.c, which might cause confusion in some cases, since such items were previously placed under either a subparagraph of 5D992.a or a sub-paragraph of 5D992.b. As mentioned above, Mass Market items that are 64 bit or less, which used to be eligible for export under 5D992 upon e-mail notification to BIS, can now be self-classified without such notification or formal classification by BIS. Mass Market items with symmetric key lengths over t64 bits (or with asymmetric algorithms over 512 bits, or elliptic curve algorithms over 112 bits) still require review and classification by BIS to confirm Mass Market eligibility.

The rule also eliminated former 5D992.c, which covered items with cryptographic functionality limited to anti-malware functionality. Such items are decontrolled and are now classified as EAR99.

BIS included a minor roll-back and potential major annoyance in its revision to EAR 742.15 by stating that items submitted for Mass Market review are no longer eligible for export under 5A992/5D992/5E992 during the 30-day waiting period. They now remain subject to control under 5X002 during the waiting period, but are eligible for export to government and non-government end-users worldwide (exc. E:1) under ENC during a 30-day period per ENC 740.1 7(b)( 1 )(i). While this has no net effect on the exportability of the items during the waiting period, it creates additional burdens to exporters managing and properly documenting exports during the waiting period. For instance, if a company is using a new version of a mass market item that needs review, the new version will have to be classified under ECCN 5X002 ENC-U for 30 days, and then reclassified *5X992* NLR in the company's Export Management computer systems and documentation. The company may also need to explain the reason for these changes in ECCN to foreign customers, especially those in countries where there is no equivalent to ECCN 5A992/5D992/5E992, and where 5A002/5D002/5E002 classification is limited only to the most sensitive encryption items and thus subject to licensing requirements.

We recommend that exporters submit comments that this process is adding needless complication rather than simplifying.

Another potential area of confusion resulting from this change is a former specific reference in EAR Part 742.15 of an exemption to ship 5A992/5D992/5E992 Mass Market items to U.S. subsidiaries and LFZ headquartered companies. This exemption mirrors similar exemptions in License Exception ENC for 5A002/5D002/5E002 items and was made redundant by the change that keeps Mass Market items undergoing review controlled at the "002" level. Exporters should be assured they can still use the U.S. subsidiary and LFZ headquartered entities exemptions for putative Mass Market items.

BIS also amended the Mass Market provisions of EAR 742.15 to eliminate the need to submit a Mass Market classification request for items using **"ancillary cryptography" and "personal area network" items,** as discussed above in relation to License Exception ENC. Thus, if an exporter is comfortable making this self-classification, they may do so. As with other classifications, you always have the option of seeking a formal BIS classification for such items, but this is no longer required. We are seeking classifications for when the application of these terms is not clear, but self classifying products where we feel comfortable from the definition and examples or discussions with BIS officials in doing so.

The rule also deleted references to the decontrol notes in EAR 742.15, so the section no longer gives the complete description available in the past on how to handle encryption controls. While this change comports more with the logic of other parts of EAR 742, it is less helpful to most exporters in our view. On the other hand, BIS revised and clarified the related control notes in ECCN 5A002 and cross references to there from 5D002, so that part is much easier to apply.

**1.2.6 Subsequent Bundling.** The rule removed the long standing "subsequent bundling interpretation" from EAR 770.2(n) and replaced it with reworded notes in 740.17(b) and 742.15(b). The stated purpose was to integrate the interpretation in the specific sections on encryption and to provide additional clarification concerning when a new encryption review is required. It does seem to make sense to include this interpretation as part of the core encryption provisions, but it only slightly clears up the issue of when a new review is required. The text of the new note adds language that says a new review is not required when there are “updates” to an encryption component that a program uses to provide cryptography *(e.g.* Open SSL or java components). This proves to be very helpful since such changes can include new algorithms or upgrades; however BIS reviews them all the time. The notes otherwise reinforce the interpretation that version changes do not require a new classification review, as long as the changes are not relevant to the cryptographic functionality of the product that was reviewed *(i.e.*, do not affect the Supplement 6 information). This is consistent with the long-standing BIS interpretation of subsequent bundling, but the new wording may cause some to conclude there is a difference in interpretation. We know some at BIS are scratching their heads over the wording and look forward to applying it.

**1.2.7 Removal of License Exemption KMI.** The rule removed EAR 740.8, License Exception KMI, from the regulations (along with the related Supp. No. 4 to Part 740) because BIS believes that developments in cryptography and the regulations have made it obsolete. If you are still using KMI for any products, we recommend that you consult with BIS to get a prompt ENC-U classification, because the preamble was supposed to convert such products but does not clearly do so. Key recovery systems were proposed by the U.S. government in the late 1990s as a possible structure to escrow encryption keys with the government or trusted third parties to allow government access to stored keys of encrypted data in limited circumstances, such as for law enforcement purposes. Industry and academia identified numerous problems with these systems, and they were never really broadly adopted. License Exception KMI was available for key escrow and key recovery items following a one-time review process.

**1.2.8 Encryption Licensing Arrangements. EAR** Part 742.15(a)(2) sets forth a policy for broad encryption-specific licenses called Encryption Licensing Arrangements. These licenses allow transfer of broad categories of encryption technology and software to licensed recipients without prior encryption classification review. The former language noted that ELAs are generally valid for four years, "including those which authorize exports and re-exports of encryption technology to 'strategic partners' of U.S. companies." BIS deleted the language, claiming it would add "transparency" to the policy. The deletion was presented as a sort of housekeeping measure, and BIS said it was not intended to change the policy of granting ELAs to allow U.S. and LFZ headquartered companies to export and re-export to and among "strategic partners" such as Indian contractors for product development. BIS has not adequately explained why this change makes the policy more transparent. We recommend comments to restore the policy statements on which many companies have relied for guidance.

**1.2.9 Products that Activate Dormant Cryptography.** BIS removed some explanatory language regarding controls over items that activate otherwise dormant encryption, but did not really clarify the long standing but unpublished and therefore shifting "dormant crypto rule." The revised provisions simply state that encryption controls apply to the "key" that turns on encryption functionality that has been disabled. (This is really the corollary to the dormant crypto rule, which allowed exporters to treat a crypto product, the cryptographic functions of which were not accessible, as if it did not have such functions, but only so long as they treated the enabling mechanism as if it were an export of the fully functional item.) The deletions seem to be housekeeping measures, intended to eliminate references to particular review and classification procedures. It is possible; however, that these changes could result in some additional flexibility in BIS's dealing with "dormant" cryptography where there is no intention or capability to enable the cryptographic functionality of a "dormant" or "disabled" cryptographic item. Recently, BIS and NSA have been reluctant to issue a non-Category 5, Part 2, classification for an item that has permanently disabled encryption components, such as, an encryption capable microchip that has been permanently disabled due to the lack of necessary firmware. Perhaps this is an opportunity to rationalize that tendency and return to past practice regarding dormant/disabled encryption items.

**1.2.10 No Comment Period Specified.** BIS issued this as an "interim final rule," which means it is effective immediately, and comments are invited to improve it. No comment period was specified, so it is not clear how receptive BIS and other agencies will be to comments. However, we do recommend that exporters and trade associations prepare and submit comments to improve this rule, clean up errors, and take the next step forward towards more fundamental encryption reform. Comments are one vehicle to press the Administration forward because they are required to consider comments that are provided by interested parties. In the meantime, industry groups are meeting with high level officials in the new Administration and lobbying for real reform.

**1.3 *De Minimis* Rule Clarified and Rationalized at Long Last.** On October 1, 2008, BIS issued an interim final rule revising and clarifying the *de minimis* rule, which explains when non-U.S.-made items are not subject to the EAR. The new rule, *"De Minimis* U.S. Content in Foreign Made Items," was published in 73 *Fed. Reg.* 56964 (Oct. 1, 2008).) This rule allows persons performing *de minimis* calculations to treat most (but not all) software as a part of hardware with which it is "bundled" (rather than forcing separate software to software and hardware to hardware calculations). For example, when a U.S. software provider licenses its software to a major international automobile manufacturer, the provider no longer needs to tell the customer he and his customers cannot sell their cars worldwide just because of a small amount of software that was incorporated into the car, not into other non-U.S. software. Second, the rule removed the requirement to file a one-time report before a non-U.S. company could rely on the *de minimis* rule for software. (Such reports are still required for technology.) Third, the rule clarified other aspects of the *de minimis* rule and how to perform calculations.

A little background is in order. The United States asserts that our export controls will apply not only to U.S. exports, but also extraterritorially to re-exports of U.S.-origin products and to re-exports of U.S.-origin parts and components contained within non-U.S.-origin products. That extraterritorial assertion of U.S. jurisdiction has long rankled allied countries, which believe that U.S. laws should stop at the U.S. border (as the jurisdiction of all other countries does). In the 1980s, after President Reagan imposed foreign policy export controls on transactions dealing with the trans-Siberian pipeline which was to bring oil and gas to Eastern Europe, European allies revolted. The EU and many members and other countries issued blocking statutes prohibiting European companies from complying with U.S. re-export controls, and several court cases were instituted in Europe and the United States challenging the legality of U.S. extraterritorial jurisdiction under national laws and international law. (The American Bar Association Committee on Export Controls and Sanctions has written a Resolution and accompanying Report explaining to policy makers why such assertion is not good law or policy.) Companies were actively "designing out" U.S. parts and components from their products.

This "trade war" reached the highest levels of government. Ultimately, the U.S. withdrew the pipeline sanctions and ameliorated excessive extraterritorial controls by treating subsidiaries of U.S. companies that were organized under another country’s law

as other than a "U.S. person" (under most laws) and by creating the *de minimis* rule to exempt from re-export controls most items made with 10 percent or less U.S. content (25 percent to all countries except those in Country Group E). Thus, the *de minimis* rule has served as an important safety valve to relieve some pressure against extraterritorial U.S. re-export controls and to dampen the desires of allies to "design out" U.S. parts and components. It thus preserves respect for U.S. re-export controls simply by not applying them to the nth degree. EAR 734.4 and Supplement No. 2 to EAR Part 734 have set out the *de minimis* rule and instructions for performing calculations to determine whether a product is not subject to the EAR. Those applying the *de minimis* rule are usually those who are most careful to comply with U.S. re-export controls.

The first thing that the revised rule does is to allow most software **"bundled" with hardware to be treated as a part or component for *de minimis* calculations.** Unfortunately, it limits what software can be treated as a component of hardware, bundled with the hardware, to ECCNs classified as XX99X (AT only controlled items) and EAR99 items. The agencies were too nervous to include all software and could not articulate what they thought should be excluded that was not already excluded. **We recommend that anyone submitting comments should state that all software should be eligible for bundling other than those items already excluded from the *de minimis* rule. At minimum, software classified under ECCN 5D002 but eligible for export under License Exceptions TSU or ENC-Unrestricted to all but the AT-controlled countries should be eligible given that those License Exceptions effectively treat them as AT only controlled.** Particularly, it makes no sense to treat such items as ineligible for the 25 percent *de minimis* rule because they would not be counted in any calculations anyway since they do not require a license except to AT-only controlled destinations (currently Cuba, Iran, North Korea, Sudan and Syria).

This distinction means, for example, that Windows XP, Vista, and other mass market products can be calculated as bundled into hardware just like other parts, but Linux, Windows CE, Windows XP Embedded, and other similar products cannot be because BIS/NSA consider those products not to be mass market eligible. In order for products not eligible to be treated as components of hardware, the exporter must revert to software-to-software, hardware-to-hardware, or technology-to-technology *de minimis* calculations.

Second, the rule **eliminated the requirement to file one-time reports for software** to qualify for *de minimis.* That is good news because otherwise, products clearly eligible for *de minimis* treatment would not qualify if no one had ever made a report. However, caution is advised because it means companies must perform their own calculations and stand behind them with no backing from the government review. The rule specifically warns of **record keeping** requirements in order to demonstrate that the *de minimis* rule applies. **Thus, we advise clients who use our model form of "one-time report" to continue using it (but just for your files) to document your own *de minimis* calculations.** Of course, as with all other aspects of the EAR, exporters may seek advisory opinions from BIS either formally pursuant to EAR 748.3(c) or informally

(remembering the admonition that oral advice is worth the paper on which it is written). Few one-time reports have been filed for technology, so the **requirement to file one-time reports for commingled technology has been retained.**

Finally, the rule streamlined many aspects of calculations, starting with **"what is a part."** The old rule simply gave one example, stating that a peripheral that is simply rack mounted or cable connected could not be considered "a part." However, BIS advised that telecommunications systems, for example, with components simply cable connected, could be treated as one system for *de minimis* purposes if each was an essential part and not the "principal element." The revised rule incorporates those advisories by stating that a part must be **"incorporated"** into the foreign made item, meaning the "U.S.-origin controlled item is: Essential to the functioning of the foreign equipment; customarily included in sales of the foreign equipment; and re-exported with the foreign produced item."

U.S.-origin EAR99 or XX99X classified software may be considered **"bundled"** into non-U.S.-origin hardware if it is "re-exported together with the item and is configured for the item, but is not necessarily physically incorporated into the item." A good example of unincorporated bundled software is a printer driver delivered on disk with the printer.

The calculation for *de minimis* is:

Value of the U.S.-origin Controlled Content (Fair Market Value if different from Selling Price)
divided by Fair Market Value of Non-U.S. Made Product in Market Where It Is Sold

Do not consider as part of U.S.-origin content any such content that may be re-exported to the destination in question with No License Required or under License Exception GBS. Please note that this exclusion from the scope of the EAR does not apply to the following products: (1) shipments to a Computer Tier 3 destination (as defined in EAR § 742.12) of computers exceeding a Weighted Tera FLOPS rate greater than or equal to 0.75 that contain U.S. origin semiconductors (other than memory circuits) controlled under ECCN 3AOOl; (2) shipments to a Computer Tier 4 destination (as defined in EAR § 742.12) of computers exceeding 0.002 WT containing U.S. origin semiconductors (other than memory circuits) classified under 3A001 or high speed interconnect devices controlled under ECCN 4A994.j; (3) encryption items controlled for "El" reasons under ECCNs 5A002, 5D002 or 5E002, except those that have been made eligible after notification or review for License Exception TSU, ENC-Unrestricted or Mass Market treatment; (4) specified commercial standby instrument systems integrating QRS 11-00100-1 00/10 1 Micro-machined Angular Rate Sensors.

The application of the *de minimis* rules will, of course, be technical and result in other nuanced questions, but we believe this rule clears up many long standing questions and is much cleaner and less cumbersome to apply than in the past.

(Besides the restriction on what software may be treated as bundled, we believe the fundamentals of the rule should focus U.S. jurisdiction on the U.S.-origin items in non-U.S. origin items, as has long been the case. This rule claims jurisdiction over the whole end-item because it contains U.S. content, which seems over-reaching.)

One last note, some believe this rule is different from OFAC rules. However, our view is that, for the most part, OFAC sanctions rules have a *de minimis* rule but do not explain how to calculate it. We find the explanation in the EAR far more useful to interpret and not in contradiction to OFAC rules on *de minimis* with one exception. The Iranian Transaction Regulations (31 C.F.R. Part 560) treat an item as *de minimis* if it has less than 10 percent or less for Iran, whereas all other rules are 10 percent or less. But, we have never found a single item to be precisely 10 percent U.S. content. This appears to be a distinction without a difference. However, exporters should be careful to ensure that their non-U.S. *de minimis* transactions are not captured by controls on "U.S. person" facilitation.

**1.4 BIS Amends EAR to Expand Scope of Reasons Allowing Listing of Parties on Entity List; Moves Parties from General Order No. 3 to Entity List; Adds Other Parties to Entity List**. On August 21, 2008, BIS amended the EAR to expand the scope of reasons for which BIS may add a party to the Entity List. (73 *Fed. Reg.* 49311 (Aug. 21, 2008).) **The final rule is very similar to BIS's June *5*, 2007 proposed rule on the same matter**.

The Entity List is a means by which BIS informs exporters that licenses are required for export to certain end-users of all or some items subject to the EAR because the end-user poses a risk of unlawful end-uses. Before the August 21, 2008 final rule, BIS could place a party on the Entity List to inform exporters that licenses are required for exports, re-exports or in-country transfers to said party for the reasons addressed in EAR 744.2 (nuclear end-uses), 744.3 (missile end-uses), 744.4 (chemical and biological weapons end-uses), 744.6 (proliferation-related activities of U.S. persons), 744.10 (certain entities in Russia), 744.17 (general purpose microprocessors for military end-uses/users), 744.20 (entities sanctioned by State Department), or 744.21 (military end-uses in China).

Under the August 21, 2008 final rule, BIS can list even more parties under the new broader and vaguer standard of a reasonable cause to believe, based on specific and articulable facts, that the party has been involved, is involved, or poses a significant risk of being or becoming involved in activities that are contrary to the national security or foreign policy interests of the United States, or is acting on behalf of such parties. The activities at issue do not even need to involve items subject to the EAR in order for an entity to be listed. U.S. persons, as defined by EAR 772.1, however, cannot be listed on the Entity List under EAR 744.11. EAR 744. 11(b) provides the following illustrative examples of activities that could be contrary to U.S. national security or foreign policy interests:

(1) Supporting persons engaged in acts of terror;

(2) Actions that could enhance the military capability of, or the ability to support terrorism of, governments that have been designated by the Secretary of State as having repeatedly provided support for acts of international terrorism;

(3) Transferring, developing, servicing, repairing or producing conventional weapons in a manner that is contrary to United States national security or foreign policy interests or enabling such transfer, service, repair, development or production by supplying parts, components, technology or financing for such activity;

(4) Preventing accomplishment of an end use check conducted by or on behalf of BIS or the Directorate of Defense Trade Controls of the Department of State by precluding access to, refusing to provide information about, or providing false or misleading information about parties to the transaction or the item to be checked. The conduct in this example includes expressly refusing to permit a check, providing false or misleading information, or engaging in dilatory or evasive conduct that effectively prevents the check from occurring or makes the check inaccurate or useless. A nexus between the conduct of the party to be listed and the failure to produce a complete, accurate and useful check is required, even though an express refusal by the party to be listed is not required; or

(5) Engaging in conduct that poses a risk of violating the EAR when such conduct raises sufficient concern that the End-User Review committee believes that prior review of exports or re-exports involving the party and the possible imposition of license conditions or license denial enhances BIS's ability to prevent violations of the EAR.

BIS's expansion of the scope of the Entity List was precipitated in part by the Mayrow General Trading case (*Mayrow*). In this case, BIS realized that it did not have legal authority to put Mayrow and related parties on the Entity List or the Denied Persons List but felt it important to prevent exports to them on the belief that Mayrow and related parties were transshipping parts for Improvised Explosive Devices (IED5) through the UAE to Iran for use against U.S. troops in Iraq. As a result, BIS amended the EAR on June *5*, 2006, to create General Order 3 imposing a license requirement on exports and re-exports of all items subject to the EAR to *Mayrow*: and related entities. (71 Fed. Reg. 32272 (June 5, 2006)) Again, BIS expanded General Order 3 on September 6, 2006 (71 Fed. Reg. 52426 (Sept. 6, 2006)), and then again on June 8, 2007 (72 Fed. Reg. 31717 (June 8, 2007)), to include other entities related to *Mayrow* and others that have supplied or may supply components for IEDs.

Based on the new authority, BIS amended the EAR to move all parties in General Order 3 to the Entity List and remove General Order No. 3. (73 *Fed. Reg.* 54499 (Sept. 22, 2008)) HIS also added some 75 other persons and entities to the Entity List for their acquisition or attempted acquisition of IEDs. Newly added parties are located in Canada,

China (including Hong Kong), Egypt, Germany, Iran, Kuwait, Lebanon, Malaysia, Singapore, South Korea, Syria and United Arab Emirates; based on an interagency investigation involving the Office of Export Enforcement Miami Field Office and the FBI. A grand jury also criminally indicted 16 of these entities and individuals.

Many exporters have asked BIS for clearer notice of entities that the U.S. Government knows present a risk of diversion, so this is an example of being careful what you ask for. BIS warned exporters of low level components that they need to remain vigilant about nefarious end-uses-even if not in weapons of mass destruction activities. Frankly, for those types of components which are sold through distributors, the end-users and end-uses are extremely difficult to police. Listing the parties is helpful, although it will now be a strict liability violation to sell to these new parties.

In a somewhat related matter continuing the theme of providing more information on nefarious end-users, BIS also put out guidance on how to avoid diversions to Iran's nuclear weapons related activities, which does not affect most U.S. exporters.

The August 21, 2008 rule also revised the EAR to establish procedures for listed entities to request that their listing be removed or modified. The End-User Review Committee (created for VEU) will review requests to add such entities to or remove them from the Entity List in Accordance with the procedures set forth in Supplement No. *5* to EAR 744. BIS added Supplement *5* to the final rule in response to public comments that more information needed to be disclosed on the process for adding and removing parties from the Entity List. Created in 2007. The End-User Review Committee is chaired by the Commerce Department (currently Karen Nies-Vogel) and also consists of representatives of State, Defense, Energy and, where appropriate, Treasury. It will be easier to add parties to the Entity List than to remove or modify entries because decisions to add a party can be made by majority vote, but decisions to delete the names must be made by unanimous vote (giving every agency a veto). The procedure offends traditional notions of due process, which is probably why U.S. persons will not be listed.

In response to public comments to provide guidance whether parties related to listed parties are also caught, BIS stated that it would publish guidance in the near future. BIS's position is that it believes that decisions to list or refrain from listing a subordinate or affiliated entity should be made on a case-by-case basis by the End-User Review Committee.

### 1.5 **Commerce Control List Changes**.

**1.5.1 BIS Amends EAR to Implement Wassenaar 2007 Changes**. On October 14, 2008, BIS amended the Commerce Control List (CCL) to implement changes made by the Wassenaar Arrangement to its Dual-Use Control List at its 2007 Plenary. 73 Fed. Reg. 60910 (Oct. 14, 2008) The October 14 rule also implements modifications concerning solar cells that were made by the Wassenaar Arrangement in 2006. The rule was effective October 14, 2008. If you have not already done so, review these changes

carefully, revise your export product matrices to indicate any new controls or releases from control applicable to your products, and revise your procedures accordingly.

Following are some of the more important changes made by the October 14, 2008, rule:

- ECCN 1A004.a: Expanded controls on gas masks, filter canisters and decontamination equipment and specially designed components, to cover such items designed or modified for defense against certain riot control agents.
- lAOO6: Added new ECCN to control equipment and related items that are specially designed or modified for the disposal of improvised explosive devices.
- 1A007: Added new ECCN to control equipment and devices specially designed to initiate charges and devices containing energetic materials, by electrical means.
- 2B002.c: Revised controls on optical finishing machine tools by changing number of axes (which can be coordinated simultaneously for contouring control) from three to four.
- 3AOOl.c: Modernized control levels for acoustic wave devices in c.l.a, c.l.b, c.l.c.3, and c.2.
- 3A001.e.4: Created 3AOOl.e.4 to list explicitly cover certain solar cells, cell-interconnect cover glass assemblies, solar panels, and solar arrays.
- 3A002.g: Expanded controls on atomic frequency standards.
- 3C002.e: Created 3C002.e to control all resists designed or optimized for use with certain imprint lithography equipment.
- 3C005: Expanded controls to cover gallium nitride substrates, aluminum nitride substrates, and aluminum gallium nitride substrates (in addition to silicon carbide substrates which were already controlled by ECCN 3C005) having resistivites greater than 10,000 ohm-cm at 20 degrees Celsius and to cover ingots, boules, or other performs of any of the foregoing materials with such resistivities.
- 3C006: Created 3C006 to control 3C005 substrates with at least one epitaxial layer of silicon carbide, gallium nitride, aluminum nitride or aluminum gallium nitride.
- 5A001.b: Expanded controls on underwater communications systems.
- 5A002: Revised paragraph e to Note to clarify that portable handheld devices (e.g., 3G cellular phones) providing secure Web browser, e-mail or other encryption capability across networks are controlled by 5A002, unless they qualify for 5A992 on other grounds (e.g., BIS provides a mass market encryption classification). Added paragraph g to Note to exclude from 5A002 certain portable or mobile radio telephones and similar client wireless devices for civil use. These revisions to the Note to 5A002 also

affect controls on software with encryption under 5D002's cross-reference to the Note.

- 9A012.b.4: Created 9A012.b.4 to control air breathing reciprocating or rotary internal combustion type engines specially designed or modified to propel unmanned aerial vehicles above 50,000 feet.

The October 14, 2008 rule did not implement all Wassenaar 2007 Dual-Use List changes. The Wassenaar Arrangement also expanded controls on cameras in WA 6.A.3 (ECCN 6A003 is EAR equivalent) and optical sensors in WA 6.A.2 (ECCN 6A002 is EAR equivalent). A separate EAR rule will be needed to implement these revisions. This rulemaking effort is presently on hold while State and Commerce attempt to resolve export control jurisdiction issues in this often controversial product area.

As usual, BIS is pledging to work harder not to take ten months to publish regulations implementing interagency agreed upon changes next year.

**1.5.2 BIS Publishes Second Results of its Comprehensive CCL Review.** On October 6, 2008, BIS published a final rule that implemented the second phase of its three part comprehensive review of the Commerce Control List (CCL), which began in 2007. 73 Fed. Reg. 50033 (Oct. 6, 2008). This rule takes account of comments from BIS's Technical Advisory Committees and the public. The revisions in this rule include clarifications to existing controls, eliminating redundant or outdated controls, establishing more focused and rationalized controls, and adding additional controls for clarity or for consistency with international regimes. The rule was effective October 6, 2008. If you have not already done so, review these changes carefully, revise your export product matrices to indicate any changes applicable to your products, and revise your procedures accordingly.

This rule follows the first results of the CCL review, which BIS published in the Federal Register on April 18, 2008, and which contained technical corrections and clarifications that did [ELC Memo on Regulations Implementing Export Control Reform, Etc. October 24, 2008 Page 23] not require interagency clearance. (For more on the April 18, 2008 rule, see our ELC Memo of May 30, 2008.) The third phase of the CCL review concerns changes that need to be approved by international regimes (e.g., Wassenaar Arrangement) or the U.S. Congress.

Some of the most important changes made by the October 6 rule are the following:

- 4A994 (Computers and related items not controlled by 4A003 or other more stringent ECCNs):
  - Raised the control parameter on computers in 4A994.b from an APP of 0.00001 Weighted TeraFLOPS (WT) to 0.0 128 WT.
  - Raised the control parameter on equipment for "signal processing" or "image enhancement" in (f) from an APP of 0.00001 WT to 0.0128 WT.

– Deleted (c)(2)(certain electronic assemblies), (d)(certain disk drives and solid state storage equipment), (e)(input/output control units designed for use with foregoing disk drives and solid state storage equipment), (g)(certain graphics accelerators and graphics coprocessors), (h)(certain color displays and monitors), and (k)(l )(certain hybrid computers and related items).

These deleted items now fall to EAR99. This can be a slight benefit, but makes it more complex for reexporters who are trying to determine whether reexports of U.S.-origin products are exempt from OFAC reexport controls applicable only to items controlled for export in March 1995 to Iran, because they cannot simply look just to EAR99 but must also exclude from the exemption products that have been reclassified to EAR99 (for the first time since 1991).

- 4A980 (Computers for fingerprint equipment, not elsewhere specified): Added note to clarify that 4A980 does not control equipment limited to one finger and designed for user authentication or access control, an interpretation that had never been published.
- 5A99l (Telecommunications Equipment not controlled by SAOOl): Removed (b) (8), (c)(2), and (c)(4). (b)(8) controlled certain equipment providing digital "signal processing", (c)(2) controlled certain equipment with Integrated Services Digital Network functions, and (c)(4) controlled certain equipment for routing or switching “fast select” packets. These also fall to EAR99, with the same comment as made above.
- 4AlO 1 (Computers and digital differential analyzers, not controlled by 4A00 1, designed or modified for use in missiles): Added a note to 4AlOl .b to provide a definition of “radiation hardened.”

Other ECCNs that were amended include 1C350, 1C35l, 1C352, 1C353, 1C354, 1C360, lEOOl, 1E002, 2B0l8, 2B1 19, 2B350, 2B351, 4D993, 4E992, 6A995, 7DOOl, 7E001, 7E002, 7E101 and 9E101.

The October 6 rule included changes not relating to the CCL review. EAR 744.21 prohibits exports, reexports, and transfers of 744 Supp. 2 items to the People’s Republic of China without a BIS license if you know, or have been informed by BIS, that the item is intended, entirely or in part, for a military end-use in the PRC. The October 6 rule amended 744.21 to clarify that it applies only to Supp. 2 items that are subject to the EAR.

**1.6 BIS Mandates Use of SNAP-R to File License Applications, Classification. Requests, and Certain Other Submissions.** BIS issued a final rule requiring that virtually all export and license applications, classification requests, encryption review requests, License Exception AGR notifications, and accompanying documents for all of the foregoing be filed through BIS’s SNAP-R system. 73 *Fed. Reg.* 49323 (Aug. 21, 2008). Paper applications are no longer acceptable for such submissions. This

requirement does not apply to other submissions, such as applications for Special Comprehensive Licenses or Special Iraq Reconstruction Licenses, advisory opinion requests, encryption self-classification notifications (EAR 742. 1 5(b)(l), or encryption key-length increase (EAR 740.1 7(d)(3)) notifications.

The SNAP-R filing requirement was effective October 20, 2008. Applicants can now file using paper only if one of the following exceptions applies (as a practical matter, the main exception is (i)):

(i) BIS has received no more than one submission (i.e. the total number of export license applications, reexport license applications, encryption review requests, license exception AGR notifications, and classification requests) from that party in the twelve months immediately preceding its receipt of the current submission;
(ii) The party does not have access to the Internet;
(iii) BIS has rejected the party's electronic filing registration or revoked its eligibility to file electronically;
(iv) BIS has requested that the party submit a paper copy for a particular transaction; or
(v) BIS has determined that urgency, a need to implement U.S. government policy or a circumstance outside the submitting party's control justify allowing paper submissions in a particular instance.

To request authorization to file a paper application, an applicant must state in Block 24 or in an attachment to the paper application which of the SNAP-R filing exception(s) applies and provide supporting information. If BIS disagrees, it will return the paper application without action.

We have strongly recommended that companies register and use SNAP-R even before it became mandatory anyway. It saves at least one or two weeks compared to paper submissions because applications filed electronically are registered almost immediately. The applicant will also receive the BIS licenses/decision letters electronically the day they are approved. While paper copies of licenses/decision letters will still be mailed, it may delay the process an additional one to two weeks. The electronic licenses/decision letters obtained from SNAP-R are effective upon issuance.

We can provide assistance in registering for SNAP-R. BIS provides guidance on its website at http://www.bis.doc.gov/snap/pinsnapr.htm. Earlier, BIS issued a proposed rule concerning mandatory SNAP-R. 72 *Fed. Reg. 59231* (Oct. 19, 2007). The August 21, 2008 final rule makes only minor changes to the Oct. 19, 2007 proposed rule. The most important change may be exempting from the SNAP-R filing requirement applications for Special Iraq Reconstruction Licenses.

**1.7 Census Bureau Implements Mandatory Automated Export System Filing for All Shipments Requiring Shipper's Export Declaration Information**. On June 2, 2008, the U.S. Census Bureau issued a final rule to require that all export information for

which Shipper's Export Declarations (SED) are required be filed through the Automated Export System (AES). 73 *Fed. Reg.* 31548 (June 2, 2008). Mandatory AES filing has been introduced in stages. Prior to the issuance of this rule, AES filing was mandatory for all items subject to the ITAR or listed on the EAR's Commerce Control List, but paper SEDs were still acceptable for EAR99 items. Under the June 2, 2008 rule, all SEDs (now known as Electronic Export Information or EEI must be filed through AES -- even for EAR99 items. While the changes became effective on July 2, 2008, the Census Bureau did not mandate enforcement until September 30, 2008, to provide the industry sufficient time to comply with its provisions. Census officials will be performing substantial outreach to industry on FTR requirements.

The rule significantly revises Census' old Foreign Trade Statistics Regulations (FTSR) and renames them the Foreign Trade Regulations (FTR). Exporters who have not done so should review the FTR and update their procedures accordingly for filing export information and their export compliance programs. The AES filing exemptions have been revised in certain respects, but such changes apparently are only cosmetic. Census officials have stated that everything that was exempt from filing in the old FTSR is also exempt in the FTR.

The June 2, 2008, rule implements provisions in the Foreign Relations Authorization Act (Public Law 107-228), which was enacted into law in 2002. Census issued an earlier version of the rule in proposed form on February 17, 2005. 70 *Fed. Reg.* (Feb. 17, *2005)*. Issuance of the final rule was held up because of a dispute between Census and the Department of Homeland Security (DHS) concerning the sharing of export data with foreign governments and the Option 4 program. While it continues to favor sharing of such data with foreign governments to fight terrorism, DHS allowed the final rule to proceed with a prohibition on sharing AES data with foreign governments. The Option 4 program allows approved exporters to file export information up to ten calendar days after export. Despite objection from DHS that expressed concern that the program created a potential loophole that could impede enforcement, Option 4 remains in place (now known as post-departure filing) for approved users, but the suspension on accepting new users also remains in place as negotiations between the agencies continue.

The FTR also provide for higher civil penalties. Civil penalties for failure to file or late filing were increased to a maximum of $1,100 for each day of delinquency with a maxim of $10,000 per violation. Also, for other violations of the FTR (e.g., filing of false and/or misleading information), a maximum civil penalty of $10,000 can be imposed per violation. The FTR also provide that the maximum criminal penalty for each filing violation made knowingly is a $10,000 fine or imprisonment for no more than five years or both. (We understand that the said criminal penalties have been effective since the enactment of Public Law 107-228.) In the past, the maximum penalty for most civil violations under the old FTSR was $1,000 per violation and never enforced. The June 2 rule provides for the enforcement of the FTR by the BIS' Office of Export Enforcement (OEE) and DHS's Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) as well as by Census. Customs is authorized to enforce

the FTR at the borders. OEE is authorized to enforce in cases that it brings, or when requested by Census. Census' practice is to work with exporters towards achieving informed compliance *(85-95 percent)*, but if the exporter does not cooperate, or the matter is more serious, they will refer cases to OEE for more rigorous enforcement since Census has no enforcement branch.

The FTR contain provisions for the filing of voluntary disclosures, which in practice apply when the procedure for correcting AES filings is not available. (Census officials have said if errors can be corrected, generally within 90 days of departure, it is usually sufficient for the exporter to correct the AES records as provided by the FTR. If not, consider filing a voluntary disclosure.) The FTR's voluntary disclosure provisions are similar to the EAR's voluntary disclosure provisions. The FTR's voluntary disclosure provisions state that Census will notify OEE, CBP, and ICE about **all** voluntary disclosures and will refer matters, if necessary, to the OEE. Census officials have stated that they will recommend that OEE prosecute only the most egregious cases of noncompliance, and OEE officials have said they have sufficient workload not to want to pursue minor paperwork violations. However, Census officials have also stated that parties making four voluntary disclosures in three years for the same offense will not receive the benefit of mitigation for the fourth voluntary disclosure.

In the area of routed transactions, the FTR require an agent of a Foreign Principal Party in Interest (FPPI), upon request, to provide to the USPPI a copy of the agent's power of attorney or written authorization to file the EEl on behalf of the FPPI, before the USPPI provides the required export information to the agent to prepare the EEl. The FTR also requires such agent to provide the USPPI with certain data elements filed through the AES, which will better enable the USPPI to verify that the agent has filed the USPPI-provided information accurately. These requirements existed under the old FTSR, but were not clear, and caused a fair amount of confusion in the forwarding industry. The FTR also clarify that the USPPI can file AES on behalf of the FPPI if authorized to do so.

The appendices to the FTR include a sample power of attorney and a sample written authorization that parties can execute to authorize others to prepare or transmit electronic export information, ABS filing codes, summary of exemptions and exclusions from EEl filing, and a concordance chart between the provisions of the old FTSR and the FTR.

### 1.8 Additional Issues of Note

- BIS has invited companies to submit e-mails to CommodityClassification (d~bis.doc.gov to request BIS to make links available on its web site of company classification data so that exporters will have one place to go for such links. Companies should provide: 1) company name, 2) general description of the products/services, 3) commodity classification information website address, and 4) export control point of contact.

- The Emerging Technology and Research Advisory Committee has had its initial meeting to begin consideration of the Deemed Export Advisory Committee Report and comments from exporters (we assisted on some) on that Report's proposals to limit the scope of technologies, subject to the deemed export rule, but perhaps expand the poo1 of persons subject to deemed export licensing requirements. Their important work in this area is just getting started.
- BIS added Kosovo to the EAR under Country Group B among other things. 73 *Fed. Reg.* 512.17 (Sept. 2, 2008).
- BIS issues minor changes to regulations on chemical and biological weapons related controls by revising controls on animal pathogens and adding Guinea Bissau and Republic of the Congo as States Parties to the Chemical and Biological Weapons Convention. 73 *Fed. Reg.* 38908 (July 8, 2008).
- AEA submitted comments on which we assisted on Conforming Changes to Certain End-User/End-Use Based Controls in the EAR; Clarification of the Term "Transfer" and Related Terms as Used in the EAR, which focused on the recent trend to increase controls on in-country transfers, which is unenforceable by exporters or the government but an increasing trap for the unwary.
- BIS is making more online training tools and power points available on its web site.

## 2. Defense Export Control Developments

There have been fewer developments of note with regard to ITAR compliance. While Presidential Directive 56 required reform of ITAR licensing, that has largely been interpreted by the State Department as a requirement to speed up processing of license applications, agreements, and commodity jurisdiction requests. While the increased efficiency is quite helpful in many cases, DDTC has gone to extremes in returning cases without action if it would take longer than the new timelines allow to process the files. This is a false time savings. Further reform of commodity jurisdiction decisions will require changes in personnel at the policy level or an additional push.

**2.1 Increases in ITAR Registration Fees.** After limiting the registration period to one year for all registrants in July, the Directorate of Defense Trade Controls published a final rule on September 25, 2008 instituting a new fee schedule for all registrants (i.e., manufacturers, exporters, and brokers). See 73 *Fed. Reg.* 55439 (Sept. *25*, 2008) Registration fees will now start $2,250 per year and rise depending on the number of authorizations (e.g., licenses and agreements) approved by DDTC in the previous year. For companies with a large number of authorizations per year, the rise in fees could be dramatic.

DDTC states that it is adopting the new fee structure "to better align registration fees with the cost of licensing, compliance and other related activities e. g. commodity jurisdictions and to meet the requirements of the President's National Security Directive-

[56] on Export Control Reform." In other words, more personnel for licensing and prosecuting enforcement cases.

The new fee structure is broken down into the following three tiers:

- $2,250 for new registrants and those registrants for whom DDTC has not reviewed, adjudicated, or issued a response to any applications with the previous year. (i.e., the twelve-month period ending 90 days prior to the expiration of their registration).
- For those registrants where DDTC reviewed, adjudicated, or issued between one and ten application in the previous year, the new fee with be $2,750.
- For those registrants where DDTC reviewed, adjudicated, or issued over ten applications in the previous year, the new registration fee will be $2,750 plus $250 for each application over ten. For Tier 3 registrants whose total registration fee exceeds three percent of the total value of applications processed by DDTC, their fees will be capped at three percent of the value of all such applications or $2,750 whichever is greater.

Applications that count toward registration fees include all licenses (including amendments) and agreements (including amendments). Cases that are returned without action or denied do not count towards the calculation of registration fees. Voluntary disclosures, commodity jurisdiction requests, and submissions that do not require a response from DDTC (e.g., sales reports) do not count.

Non-profits, such as universities, can apply to have their fees reduced to Tier 1.

Expect a letter from DDTC at least 60 days prior to the end of your current registration notifying you of your new rate. If you fail to receive a letter, you can contact DDTC for the calculation. If you disagree with DDTC's calculation, you may submit a challenge with your renewal package, so long as you pay the minimum fee of $2,250 at that time.

**2.2 DDTC Issues Final Rule Concerning FAA Certified Parts and Components.** On August 14, 2008, the Directorate of Defense Trade Controls (DDTC) published a proposed rule clarifying the application of Section 17(c) of the Export Administration Act (EAA) to civil aircraft parts and components 73 *Fed Reg.* 47,523 (Aug. 14, 2008). After reviewing more than 20 comments from industry on the proposed rule published by DDTC on April 11, 2008 *(see* ELC Memorandum of May 30, 2008), DDTC issued the final rule in substantially the same form.

The final rule creates a Note to U.S. Munitions List Category VIII(h) that provides that civil aircraft parts and components are not subject to jurisdiction under the ITAR if such part or component is:

(a) standard equipment;

(b) covered by a civil aircraft type certificate (including amended type certificates and supplemental type certificates) issued by the [FAA] for civil, non-military aircraft (this expressly excludes military aircraft certified as restricted and any type certification of Military Commercial Derivative Aircraft, defined by FAA Order 8110.101 effective date of September 7, 2007 as "civil procured or acquired by the military");
(c) an integral part of such civil aircraft; and
(d) not Significant Military Equipment (SME) under the ITAR.

If any doubt exists as to the above criteria, the rule states that a formal commodity jurisdiction is required.

"Standard equipment" is defined as a "part of component manufactured in compliance with an established and published industry specification industry specification or an established and published government specification (e.g., AN, MS, NAS or SAE). Parts and components that are manufactured and tested to establish but unpublished civil aviation industry specifications and standards are also 'standard equipment,' e.g., pumps, actuators, and generators. DDTC included unpublished specifications and standards in response to industry concerns that limiting the rule to published materials did not take into account that many aerospace specifications and standards go unpublished to protect intellectual property rights of the manufacturers.

The proposed rule also clarifies that simply testing a part or component to a military standard does not mean that it does not qualify as "standard equipment," unless the part of component was designed or modified to meet the military specification. Industry often tests civil parts and components to military specifications for marketing purposes.

The final rule defines "integral" as "a part of component that is installed in an aircraft." In determining whether a part or component may be considered as standard equipment and integral to a civil aircraft (e.g., latches, fasteners, grommets, and switches) it is important to review carefully all of the criteria noted above. For example a part approved solely on a noninterference/provisions basis under a type certificate issued by the [FAA] would not qualify. Similarly, unique application parts or components not integral to the aircraft would also not qualify.

Despite objections from ten commentators, the new rule does revise U.S. Munitions List Category VIII to add military hot section engine components and military digital engine controls to Category VIII(b), which makes them SME. Therefore, military hot section engine components and military digital engine controls are not eligible for the self-CJ provisions of the new rule, unless the SME part or component was integral to civil aircraft prior to August 14, 2008. DDTC reasons that requiring CJ's for military hot section engine components and military digital engine controls will help "ensure that the U.S. Government is made aware of and can reach an informed decision regarding any sensitive military item proposed for standardization in the commercial aircraft before the item or technology is actually applied to a commercial aircraft program." The new rule

made the following two minor concessions: (1) the rule exempts military hot section and digital engine controls parts and components manufactured to design drawings dated prior to January 1, 1970; and (2) DDTC will not require DSP-83 Non-transfer and Use Certificates for the export of spare parts for hot sections and digital engine controls for previously authorized exports.

**2.3 DDTC Changes to Licensing of Foreign Person Employees.** DDTC issues an update to its policy regarding licensing of foreign person employees of U.S. companies who have access to ITAR-controlled data and services as part of their job. DDTC has eliminated the redundancy of having both a DSP-5 license and a Technical Assistance Agreement (TAA) in place to cover a foreign persons' employment and related activities.

Now, U.S. companies need only obtain a DSP-5 license to authorize the transfer of technical data and defense services to their foreign person employees. A foreign person employee may be located in the United States or overseas, so long as the employee is a "full time regular employee who is directly paid, insured, hired, fired and/or promoted exclusively by the [U.S. company]." The DSP-5 license application must specifically state in block 20 that it is "[f]or employment of a foreign person who will require access to technical data related to [name of program/commodity]." The following supporting documents must be attached to the license application: (1) cover letter explaining the requirement and scope of employment; (2) copy of passport and work authorization; (3) resume; (4) job description; (5) detained description of technical data to be released and copies of such data as necessary; (6) non-disclosure agreement (a template is provided on DDTC's website); (7) the company's Technology Control Plan; and (8) a DSP-83 for applications involving SME or classified items. DDTC has created a sample checklist for completing a DSP-5 application for foreign national employees, found at http://www.pmddtc.state.gov/licensing/documents/Industry_Chesklist_dsp-5FPE.doc. The DSP-5 license will be valid for the shorter of four years or the expiration of the foreign person employee's authorization to stay in the United States.

If a foreign person is to engage in activities covered by a TAA its employer has in place, the TAA must be amended to specifically identify the foreign employee's country/countries of nationality if such countries are not already within the geographic scope of the agreement, but the foreign employee does not have to be signatory to the agreement. However, DDTC has indicated in its FAQ's related to this new policy that "the agreement holder must amend the agreement to specifically identify the foreign person employees of all U.S. signatories." The statement should be made in 22 CFR 124.7(4) with other statements regarding transfer territory. If the foreign employees are not already identified, this statement should be included in the next amendment submitted to DDTC for approval.

If you have DSP-5s and TAAs currently in place for certain foreign employees, those authorizations are still valid. Once the authorizations expire, you will be required to submit the appropriate authorization consistent with the current guidance. If you wish to immediately take advantage of this new policy, you must submit a new DSP-5 license.

Upon receipt of the the DSP-5 application, you may surrender the open DSP-5 and terminate the TAA. This new policy removes the dual licensing of the past and makes licensing of a foreign employee less complicated for U.S. employers going forward.

## 3. Embargo and Sanctions Developments

**3.1 North Korea Removed from List of State Sponsors of Terrorism, but Tight Export Controls Remain in Place.** There have been a number of front page headline developments regarding the North Korea sanctions, but no actual change in U.S. export **controls** yet. **Until the EAR is amended, virtually all exports to North Korea still require a license.** Despite the numerous press releases and official Presidential and Secretary of State determinations removing North Korea from the terrorism list (73 *Fed Reg.* 63450 (Oct. 24, 2008)), there have been only very minor changes to the sanctions with "relaxations" essentially symbolic in nature with little real effect on international trade.

The United States and North Korea met in Singapore in April 2008 to finalize a September 2007 agreement to freeze the North Korean nuclear weapons program in exchange for a relaxation of U.S. sanctions against North Korea. Following those meetings, on June 26, 2008, President Bush terminated the remaining Trading With the Enemy (TWEA) sanctions (already significantly relaxed in 2000 by the Clinton Administration), which had been in effect since 1950. *73 Fed.* Reg: 36785 Jun. 27, 2 00 8. (The only other surviving sanctions program authorized by the TWEA is OFAC's Cuban Assets Control Regulations.) However, at the same time, President Bush invoked the International Emergency Economic Powers Act (IEEPA) (the basis for all other current OFAC sanctions programs, and currently for the EAR) to maintain the current strict export controls, continue to freeze already-frozen North Korean assets, and prevent U.S. persons from dealing with North Korean flagged vessels. E.O. 13466, *73 Fed. Reg* 36787 (Jun. 27, 2008). Furthermore, a number of key North Korean entities remain on the OFAC SDN list under non-proliferation based sanctions programs and subject to target EAR license requirements. The formal termination of the TWEA sanctions on June 26, 2008, was mainly a diplomatic move, as it eliminated only prohibitions on the import of North Korean goods into the United States and restrictions on U.S. person assistance to North Korean government nuclear and missile programs (although most such activities would likely be prohibited under the Department of Energy regulations and/or the EAR and/or the ITAR). Not surprisingly, North Koreans were not mollified by being sanctioned under IEEPA rather than TWEA.

EAR dual-use export controls were tightened following an alleged North Korean nuclear test in October of 2006, which gave rise to UN Security Council Resolution 1718. These are among the strictest U.S. export controls, imposing export license requirements on all items subject to the EAR, except EAR99 food and medicine. As noted above, export-related aspects of the TWEA sanctions were suspended in 2000 and replaced with EAR-based export controls.

The United States also promised to remove North Korea from the State Department's list of state sponsors of terrorism within 45 days, in light of a statutory requirement for Congressional notification. Bush certified to Congress on June 26, 2008, that North Korea had not engaged in any acts of terrorism in the past six months, and that it had provided assurances that it would not do so in the future. *73 Fed. Reg.* 37351 (Jul. 1, 2008). The 45-day period was to have elapsed by August 11, 2008, but the U.S. delayed its implementation of this commitment until October in order to secure additional promises from North Korea not to re-activate its idled Yangbon plutonium production facility.

North Korea was placed on the state sponsors of terrorism list in 1988 due to its alleged involvement in the downing of a South Korean airliner in 1987 and other support of terrorist groups; According to the Congressional Research Service, Japan objected to the U.S. removing them from the list based on claims that North Korea has engaged in the kidnapping of Japanese citizens and that foreign governments have also linked North Korea to recent support for Hezbollah in Lebanon and the Tamil Tigers in Sri Lanka, both of which are listed on the U.S. State Department's list of foreign terrorist organizations. U.S. and Israeli governments have also alleged that North Korea to has engaged in assistance to the Syrian government - itself a designated state sponsor of terrorism related to suspected nuclear proliferation activities, resulting in the bombing of a facility in Syria in 2007 by Israel.

Notwithstanding these international objections, after North Korea restarted its nuclear power activities and threatened to remove IAEA inspectors, President Bush directed the Secretary of State on October 11, 2008 to remove North Korea from the state sponsors of terrorism list. The effect of this action was to suspend sanctions imposed pursuant to Section 6(j) of the Export Administration Act of 1979 (currently in lapse; but the EAR issued pursuant to the EAA are continued in effect by Executive Order under IEEPA as if the EAA were still in effect), Section 40A of the Arms Export Control Act, and Section 620A of the Foreign Assistance Act.

Removal of North Korea from the state sponsors of terrorism list authorizes the elimination of certain restrictions on U.S. government institutions in financial matters, including:

- Prohibitions on economic assistance from the U.S. government;
- Required U.S. opposition to loans by the World Bank and other international financial institutions;
- Prohibitions on diplomatic immunity to allow families of terrorist victims to file civil lawsuits in U.S. courts;
- Prohibitions for tax credits for income earned in terrorist-listed countries;
- Denial of duty-free treatment of goods exported to the United States;
- Authority to prohibit any U.S. person from engaging in a financial transaction with a terrorist-list government without a Treasury Department license; and

- Prohibition of Defense Department contracts above $100,000 with companies controlled by terrorist-list states.

The de-listing also removed statutory restrictions on military and dual-use export controls, but will likely have no practical effect on current EAR or ITAR export controls against North Korea. As mentioned above, EAR export controls already exceed the restrictions that result from a country being listed as a state sponsor of terrorism. This action may result in amendments to the EAR to remove terrorism related restrictions, and we understand that BIS is taking the matter under consideration, but that no action has been taken yet. It is possible that the listing could affect the consideration of license applications for export to North Korea of low-level items, such as mass market computers and encryption software, that are controlled under the EAR for anti-terrorism reasons only, and that North Korea could simply be treated as a D:1 (as well as D:2, D:3, and D:4) country, but that will require a regulator change. An EAR amendment could be more limited.

While the removal from the terrorism list also eliminates the basis for ITAR licensing restrictions under ITAR 126.1(c), ITAR 126.1(a) and 126.1(d) still impose a policy of denial of ITAR licenses, flowing from the imposition of a UN arms embargo against North Korea and various other pieces of U.S. legislation. Removal of ITAR restrictions will likely be far down the road for North Korea. In the case of Libya, comprehensive U.S. trade sanctions were lifted in April of 2004, and it was removed from the state sponsors list in June of 2006. However, Libya is still subject to an ITAR policy of denial with case by case review for non-lethal defense articles, which was only scaled back from a full arms embargo in February of 2007.

The OFAC Terrorism List Regulations, 31 C.F.R. Part *596*, which prohibit U.S. **persons from engaging in financial transactions with a Terrorism List government** will also need to be amended to drop North Korea from the list of countries affected. Perhaps this action will also stimulate OFAC to remove Iraq and Libya from the schedule of countries in these regulations since they were dropped from the state sponsors lists in 2004 and 2006, respectively, but nonetheless remain listed in the OFAC regulations.

There are still many legal obstacles before trade relations with North Korea can be normalized. On October 11, 2008, the State Department issued a fact sheet that lays out no less than nineteen other U.S. laws, regulations, or Presidential determinations that impose various types of export control, financial, and other sanctions against North Korea or North Korean entities' based on North Korea's WMD proliferation activities, human rights practices, status as a communist state, and other reasons.

**3.2 OFAC Issues New Sanctions Enforcement Guidelines.** The U.S. Treasury's Office of Foreign Assets Control (OFAC) issued a revised set of "Economic Sanctions Enforcement Guidelines" on September 8, 2008. *73 Fed. Reg.* 51933 (Sept. 8, 2008). The new Guidelines took effect when issued. Nevertheless, Treasury solicited written

comments on them through November 7, 2008. (The "American Bankers Association", NFTC, and others submitted comments).

The new Guidelines reflect continuing efforts to impose regularity on an area of sanctions enforcement that is often criticized as unpredictable. The new Guidelines mark the first published effort at broad revision since the publication in January 2003, of "proposed rules" which, though never formally adopted, were viewed informally as a guide to sanctions penalty practice until last month. OFAC reports that the new Guidelines also take the place of interim final rules issued in 2006, which were addressed to and limited to banking institutions.

According to OFAC, the new Guidelines were prompted by enactment of the Emergency Economic Powers Enhancement Act (IEEPA Enhancement Act) in October 2007, which substantially increased penalties in the IEEPA-based sanctions programs, although of course the Proposed Rule predated that by four years. Now, under the IEEPA Enhancement Act, the statutory maximum penalty for IEEPA violations can climb to as high as twice the total transaction value of $250,000 per violation. The aim of the new Guidelines is to identify factors and considerations that will go into establishing what, if any, penalties are appropriate.

Several of these aggravating and mitigating factors are much the same as they were in the Proposed Rule, having undergone little more than a few semantic changes. The way in which the factors now are applied to violations, however, is different. The new Guidelines set forth the general considerations for penalty assessment, most of which reflect differences in emphasis rather than substance. The new Guidelines announce the intention to move away from identification of specific facts (such as the existence of compliance programs and the like) to the "better practice" of identifying "General Factors" which become "part of a holistic consideration of the facts and circumstances of each particular case." 73 *Fed Reg.* 51935.

One such General Factor is whether the violation is willful or reckless, entailing questions of whether it is part of a "pattern of misconduct," whether there was "prior notice" (including whether a "Cautionary Letter" or a "Finding of Violation," described below, was previously issued), whether there was deliberate "concealment" of the violation (described broadly as an effort to "hide or purposely obfuscate" the violating conduct), and whether there was an awareness of the conduct on the part of supervisory or managerial-level staff—or whether, at a minimum, such staff should reasonably have been aware.

Another General Factor is the violator's own "awareness of conduct," which seems to merge at points with the "willful/reckless" factor: Did they know of the violation? Should they have known? How deeply was management involved? A third General Factor is "Harm to Sanctions Program Objectives," entailing consideration of the benefits derived by the sanctioned person or country, the potential for damage of U.S. foreign or economic policy, whether the activity would have been licensable under an

OFAC program, and whether the violation was motivated by humanitarian considerations.

Finally, the new Guidelines set forth several miscellaneous factors which should already be familiar to practitioners, such as the size and volume of regular business of the violator, and its commercial sophistication; past history of violations; compliance programs; remedial measures taken for the violation; cooperation with OFAC; whether the violation was of a long-standing regulation, or occurred in the context of a recently adopted sanctions program, and whether to make an example of the violator, for the education of others in the market sector. Much of this, of course, will appear to be slightly newer bottles for the same beverage. It is important, however, that the regulated learn to adopt the new language of the regulator when negotiating what penalty is appropriate or making a voluntary disclosure. From the Guidelines, the more subjective considerations of the violator's willfulness, knowledge, sophistication, and economic size seem to predominate, but future OFAC practice could vary from these appearances.

By applying the above General Factors, OFAC will now make an important new type of determination as to whether a violation rises to the level of "egregious." From that determination, OFAC will calculate a "base penalty."

In the worst sort of "egregious" cases, cases where there was no voluntary disclosure, OFAC can set a base penalty of the statutory maximum penalty under the Enhancement Act, double the value of the underlying transaction or $25,000, whichever is higher. A voluntary disclosure will reduce the maximum base penalty to a sum approximately equal to half the value of the transaction, essentially a 50 percent deduction.

In "non-egregious" cases where the violator did not voluntarily disclose, an "applicable schedule amount" will be imposed as the base penalty. In such cases, OFAC will fix the base penalty according to a "schedule" of incremental bands set forth in the new Guidelines. If the value of the transaction underlying the violation falls within a certain band, the base penalty level will be the top value of that band. These bands are fixed at $1,000, $10,000, $25,000, $50,000, $100,000, and $170,000, and, for any transactions over $170,000, the based penalty is capped at $250,000. (Thus, if OFAC determines that the value of a transaction is $40,000, the base penalty will be $50,000; if it determines that it is $200,000, the penalty will be $250,000, if it determines that it is $1,000,000, the penalty still will be $250,000.) A voluntary disclosed "egregious" violation could result in a lower base penalty than a non-egregious violation that was not disclosed. In contrast, if voluntary disclosure had occurred, OFAC will assess a base penalty of half the transaction amount (not half the fixed penalty), capped at $125,000. (Some practitioners have pointed out that this is roughly the same as the penalty that would have been imposed, before the new Guidelines, for self-reported violations.)

Once these base penalties have been set, they can be subject to significant offsets. Where there was no voluntary disclosure, but the violator has shown substantial cooperation, the above penalties can be reduced by 25 percent to 40 percent—and by

even more than that if there was voluntary disclosure. Additionally, first-time violation penalties can be reduced by up to 25 percent, depending on whether there had been a prior "caution" or "warning." However, the traditional rule of applying only a five-year "look back period" for prior violations (without taking into account those older than five.years) reportedly only applies now to banks, not to other companies. The impact of past penalties does not expire with the statute of limitations. This may be an oversight, and we advise those commenting to address it.

Before the new Guidelines were promulgated, OFAC occasionally issued "warning letters" to violators, in cases where it had decided that a violation had occurred, but there was little point in imposing a penalty. Practitioners have occasionally been surprised by OFAC decisions in this regard, sometimes pleasantly, sometimes unpleasantly. It is difficult to generalize past practice, other than to say OFAC issued warning letters in far fewer than 95 percent of the voluntary disclosures submitted (as the Commerce Department practice has been), or even greater percentage (as the State Department practice has been). A violator would have been more likely to receive only a warning letter if the violation did not involve a lot of money, if there had been a voluntary disclosure, and if the violator had taken steps to correct the situation upon discovery. Warning letters were not deemed final agency actions, however, and therefore a recipient had no opportunity to respond meaningfully to OFAC's finding that a violation had occurred.

The new Guidelines continue the provision of non-penalty actions, with the use of "Cautionary Letters" and "Findings of Violations." Cautionary letters are to be issued where OFAC has found insufficient evidence of violation. Although these letters will not constitute final agency action and so will not be published, they will be copied to other federal regulatory agencies. It is a good practice for recipients to respond for the record to state their side, and to copy their regulators as well.

Where there is sufficient evidence of violation, however, but OFAC also determines that imposition of a monetary penalty would be inappropriate, OFAC now will issue a Finding of Violation. The Finding of Violation is a formal notice from OFAC that a violation has occurred, but the entity is not being penalized. In contrast to the "warning letters" of prior OFAC practice, however, a Finding of Violation does constitute final agency action, affording the violator the right to respond and appeal. It may be prudent to respond to such actions because they become part of the permanent record.

The new Guidelines also reiterate OFAC's openness to negotiated settlements.

Negotiations can be protracted, however, and OFAC states that it will ask for waivers of limitations periods where indicated in order to continue negotiation. Most companies agree to grant such waivers because negotiated settlements usually neither admit nor deny liability, and if one is not willing to waive the statute of limitations, OFAC will likely issue a penalty notice. It also points out that there are heavy penalties, up to $50,000, for failure to provide information; several thousand dollars for failure to

file reports of blocked property; and $5,000 for failure to maintain required records—and $10,000 for repeat violations.

Note that the new Guidelines, like those they supersede, do not explicitly describe how the existence of a violation is initially determined. Rather, they addressed the calculation of penalties for violations once it has been decided that the violations have in fact occurred. **The incrementally more detailed description of this calculus in the new** Guidelines might well make it easier for the practitioner to predict the amount of the penalty that would ensue from a voluntary disclosure. They shed little new light, however, on situations where one needs to predict whether OFAC will deem a violation has occurred in the first place. (In practice, we have found that OFAC does mitigate when the application of the regulations is unclear.) The lower maximum penalties in voluntary-disclosure cases, where formerly these penalties were a function only of the value of the transaction, might make voluntary disclosure a more attractive option for violators, but not one free of uncertainty and risk. Also, the newly created distinction between "egregious" and "non-egregious" violations is not unwelcome to the practitioner representing the inadvertent violator, but where the line falls between the two categories is still hard to discern.

The publication of these Guidelines is commendable and helps make decision making and factors for penalty negotiations more transparent, even though that does not result in OFAC practice always being clear.

***

We hope you find this memorandum useful. Please let us know if we can provide additional information on these or other matters affecting your business.

**Raymond F. Sullivan, Jr.**

***Shareholder***

**BAKER DONELSON BEARMAN CALDWELL & BERKOWITZ, PC**
**555 Eleventh Street NW**
**Washington D.C. 20004**
**Phone: 202-508-3466**
**Fax: 202-220-2266**

**EMAIL: rsullivan@bakerdonelson.com**