BY HAND
U.S. Department of Commerce
Bureau of Industry and Security
Regulatory Policy Division
14th & Pennsylvania Avenue, N.W.
Room 2705
Washington, DC 20230
ATTN: RIN 0694-AD29

Re: Comments on Advance Notice of Proposed Rulemaking Concerning Revision and Clarification of Deemed Export Related Regulatory Requirements

Ladies and Gentlemen:

We are writing on behalf of the Section of International Law of the American Bar association in response to the Advance Notice of Proposed Rulemaking concerning the Revision and Clarification of Deemed Export Related Regulatory Requirements published the U.S. Department of Commerce, Bureau of Industry and Security (BIS), on March 28, 2005 (70 Fed. Reg. 15607) (the “Notice”). The views expressed herein are presented on behalf of the Section of International Law. They have not been approved by the House of Delegates or the Board of Governors of the American Bar Association and, accordingly, should not be construed as representing the policy of the American Bar Association.

As outlined below, we believe the proposed changes described in the Notice would have a significant effect on the burden of the regulated community and may not be properly tailored to address the threat of terrorism and weapons proliferation the changes are designed to solve.

Moreover, we respectfully suggest that before any changes are made to the deemed export rule, a concentrated effort should be undertaken by BIS, in consultation with the other relevant national security authorities, the regulated community, academia, and the bar, to generate a consensus concerning the nature of the threat and the appropriate role of deemed export controls in response to that threat. The Section of International Law would be pleased to assist in that effort.

We are grateful to BIS and the Department of Commerce for this opportunity to provide comments. The Section of International Law, along with the exporting community, strongly supports the goal of preventing terrorism and the proliferation of weapons of mass destruction through effective controls on exports. To the extent the deemed export regulations currently further this goal, we believe that greater education of the regulated community would engender greater compliance with those regulations. But, based on our review, the proposed rules described in the Notice do not appear to be appropriate or sufficient to further the goal of effective export controls.
1. **Background**

The Notice states that BIS is reviewing the recommendations contained in the U.S. Department of Commerce, Office of Inspector General (OIG) Report entitled “Deemed Export Controls May Not Stop the Transfer of Sensitive Technology to Foreign Nationals in the U.S.” (Final Inspection Report No. IPE-16176-March 2004). In its report, the OIG concludes that existing BIS policies under the Export Administration Regulations (EAR) could enable foreign nationals from countries and entities of concern to access otherwise controlled technology. The OIG recommends certain regulatory changes that would affect existing requirements and policies for deemed export licenses.

2. **Further review is required to determine the need for any changes in deemed export licensing policy or procedure, and to establish a consensus in favor of any such changes.**

In determining the need for any change in deemed export controls, we believe it would be counterproductive to take any action not supported by a clear connection between the proposed rule and the anticipated benefit. Here, no such connection is articulated, either in the OIG report or in the BIS Notice. Any change in the rules not supported by such a showing may be susceptible to legal challenge, and my not generate adequate support from the regulated community or U.S. allies. Courts have held that agency action under the International Emergency Economic Powers Act (IEEPA) is subject to the judicial review provisions of the Administrative Procedures Act. Under this line of cases, regardless of the APA standard applicable to rulemaking under the EAR as continued under IEEPA, the proposed provisions must be supported by evidence in order to survive judicial review.

Moreover, in this circumstance, there does not appear to be any consensus in government, academia, the bar, or the regulated community that the increased deemed export controls

---


2. The EAA lapsed several times during the 1990s with the EAR being continued through Executive Order under the provisions of IEEPA. The EAA was reauthorized by Congress from November 13, 2000, through August 20, 2001, but failing a legislative agreement, lapsed thereafter. The EAR have been (and remain) continued by Executive Order 13222 of August 17, 2001, and successive Presidential Executive Orders. Consequently, the present Export Administration Regulations (EAR), including the current deemed export regime, are supported solely by Presidential Executive Order under the aegis of IEEPA.
proposed in the Notice properly addresses the threat of technology acquisition by adversaries of the United States.

Our review of publicly available materials on the threat of technology exports, and the proper response to that threat, militates in favor of a thorough study of the issue by the government, academia, the bar, and the regulated community before further steps are taken that may not properly address the threat and may not achieve the proper balance between protection of U.S. national security and the maintenance of the culture of free exchange of ideas that is one of the principal strengths of the U.S. economy. Those materials include the following: (1) the report of the 1976 Defense Science Board task force chaired by J. Fred Bucy, then-president of Texas Instruments;3 (2) a study by the National Academy of Science, which was supported by the U.S. Defense Department, among others, and chaired by Dale R. Corson, President Emeritus of Cornell University;4 (3) a follow-up report by the Corson panel addressing the issues and the steps taken by the U.S. government to implement its recommendations;5 and (4) the 1986 report of the National Academy of Sciences task force, supported by the Departments of Commerce and Defense, chaired by Lew Allen, Jr., then President of the California Institute of Technology;6

Importantly, the Allen Report concluded as follows: “The panel reviewed a substantial body of evidence – both classified and unclassified – that reveals a large and aggressive Soviet effort to target and acquire Western dual use technology through espionage, diversions, and to a lesser degree legitimate trade. There is limited but specific evidence on the means by which Soviet acquisitions are accomplished; there is also evidence to support the conclusion that such acquisitions have in some cases played an important role in upgrading or modernizing Soviet military systems. Effective, internationally coordinated export controls are necessary to counter the use of diversions and legitimate trade for such purposes. However, export controls are not a means for controlling espionage, which accounts for a high proportion of the successful and significant Soviet technology acquisition efforts. Thus, export controls must be viewed as one component in a more comprehensive program for controlling technology losses.”7

3 The 1976 report was entitled An analysis of Export Control of U.S. Technology—a DOD Perspective. This report (termed the “Bucy Report”) became the operative legislative philosophy of the 1979 Export Administration Act (“EAA”) and resulted in the creation and perpetuation of the Military Critical Technologies List (“MCTL”).


Over fifteen years have passed since the issuance of the Allen Report, and over two
decades have passed since the Corson studies, and it appears that there no longer exists a
clear consensus among the various affected parties (including government, industry,
academia, and the bar) on how best to control the exports of technology from the United
States in a rapidly changing global marketplace.\footnote{For a summary of the history of attempts to reauthorize of the EAA, see \textit{The Export Administration Act: Evolution, Provisions, and Debate}, Congressional Research Service, May 5, 2005 (RL31832).}

More recently, the Report of the Select Committee on U.S. National Security and
Military/Commercial Concerns with the People’s Republic of China (the “Cox Report”),
and the Annual Reports to Congress by the National Counterintelligence Executive
(NCIX) have expressed increased concern that foreign governments are targeting U.S.
entities for the purpose of illicit acquisition of technology for commercial and military
advantage.\footnote{E.g., the Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People’s Republic of China (the “Cox Report”, Washington, D.C., GPO 1999), Annual Reports to Congress by the National Counterintelligence Executive (NCIX) on Foreign Economic Collection and Industrial Espionage 1995- (available at www.ncix.gov).} However, both the Cox Report nor the NCIX reports focus heavily on the
threat of espionage, and nothing in those reports (nor anything in the OIG Report that is
the basis of BIS’s Notice) demonstrates that increased deemed export controls are a
proper or effective means for controlling espionage. Indeed, as noted above, the Allen
Report stated as one of its key findings that “export controls are not a means for
controlling espionage, which accounts for a high proportion of the successful and
significant” foreign technology acquisition efforts.\footnote{The Allen Report, at p. 154.}

By contrast, there are several other U.S. government activities and statutory regimes
designed to address the threat of espionage, U.S. including counterintelligence activities,
immigration enforcement, and enforcement of the Economic Espionage Act of 1986, 18
U.S.C. §§ 1831, 1832. In any event, the proper approach to the broader technology
export threat must encompass a combination of those processes, along with enhanced
education of industry and academia, in addition to strong enforcement of current deemed
export regulations.

We would also note that the NCIX annual reports also focus heavily on the acquisition
and exploitation of publicly available, public domain technology and know-how as a
major component of Chinese technology acquisition efforts. As with espionage, the
control of open source technology has never been the proper domain of export controls.

In summary, neither the Notice nor the OIG report demonstrates any compelling link
between the proposed revisions to the deemed export regulations and the threat posed by
foreign technology acquisition efforts. In these circumstances, we respectfully propose
that there should be a process of review and recommendation, prior to the BIS
rulemaking process, designed to better understand the threat posed by foreign technology
acquisition efforts, and to assess the appropriate role of export controls in fashioning a response to that threat. That review should be undertaken in consultation with BIS and the other relevant national security authorities, the regulated community, academia, and the bar. The Section would be pleased to facilitate that process in any appropriate way.

3. The Current Deemed Export Licensing Process

Under the current process, deemed export licenses are submitted to BIS, and BIS submits all such applications to three referral agencies (the Departments of Defense, Energy, and State). In addition, the Department of Commerce refers all deemed export applications to the FBI for a name check review. The OIG report states that the FBI has received derogatory “hits” based on its review of foreign nationals subject to deemed export license applications, although the nature and resolution of these derogatory “hits” is not explained.  

Also according to the OIG Report, since October 2001, the Central Intelligence Agency’s Weapons Intelligence, Nonproliferation and Arms Controls Center (WINPAC) has declined to review deemed export license applications, because of the lack of derogatory “hits” they have obtained from this exercise in the past. However, in an attempt to conduct some type of intelligence review for these applications, BIS arranged to have the CIA send BIS an updated CD-ROM of end-user reports that are connected to some element of the foreign national’s past (e.g., the university where the foreign national received his/her degree or any foreign entities which the foreign national has had contacts or association) on a monthly basis. The OIG report noted that BIS officials have not received any derogatory hits against this database since this type of review began. It is instructive that the CIA found its participation in deemed export reviews to be a poor use of its time. The proposed changes appear also to create even lower value targets for industry and an overburdened bureaucracy to chase with little expectation of a useful national security return on the investment.

Referencing earlier reports on export controls, the OIG found that compliance with deemed export regulations by U.S. companies and federal agencies remains low. However, it concluded that the reasons for noncompliance were “that the deemed export control regulations were ambiguous and deemed export control policy ill-defined.” The OIG had recommended that BIS work with the National Security Council to ensure that the deemed export control policy and regulations are clear and to not provide loopholes that could be deliberately or inadvertently be used by countries and entities to obtain controlled U.S. equipment and technologies. The OIG also recommended that BIS be more proactive and increase its outreach to high-technology companies, industry associations, and federal agencies to educate them about deemed export regulations and to help assure compliance with the deemed export rule. We commend BIS for having

---

12 Id., at 3.
13 Id., at p.6.
conducted much more extensive outreach in the last year on deemed export issues, particularly with parties that have not previously addressed the deemed export rule.

The deemed export rule was originally fashioned only in 1994 out of whole regulatory cloth and is not supported by legislative language, a fact recognized in the Congressional debates over reauthorization of the EAA. The rule did not exist during the Cold War, and no agency has shown that the nation is safer as a result of it. Nevertheless, after several years of having to deal with the current deemed export licensing system, many companies that obtain such licenses are familiar with the regime, and have implemented at some cost internal control plans in order to monitor compliance with the terms and conditions of these licenses and to restrict foreign nationals from access to equipment and technologies not authorized under license or License Exception. The proposed revisions contained in the Notice do not address the OIG’s stated goals of increased compliance with existing regulations, increased clarity of policy, and increased educational outreach.

The OIG report and the regulatory initiative described in the Notice lack any clear indication of potential diversion that would warrant changing the criteria for nationality to the country of birth criterion, a criterion not shared by any of our multilateral export control allies in the Wassenaar Arrangement. Likewise, none of our Wassenaar allies have a technology export mechanism comparable to the U.S. deemed export regime. It is common knowledge that it would be impossible for the United States to obtain agreement among the Wassenaar allies to adopt such a regime. Hence, the United States stands alone among the Wassenaar nations in erecting this form of control and will likely remain so. As a result, attempts to promulgate and enforce such rules outside the United States may not generate the support of key U.S. allies in the struggle against terrorism and proliferation and could undercut such support.

In addition to being a unilateral control that is difficult or impossible to enforce abroad, the country of birth proposal lacks an empirical basis for identifying legitimate threats to technology acquisition based on country of birth, and fails to state the basis for addressing any such threat under the aegis of export controls.

BIS licensing experience under the present deemed export regime may be illustrative in this connection. In F/Y 2004, BIS reported that it reviewed 995 deemed export license applications, representing 6% of all licenses submitted to BIS, with 70% of such licenses being for Chinese or Russian nationals. Only 8% of the deemed export applications

---

14 See, CRS Report, supra, which notes on page 15: “Deemed Exports are not expressly mentioned in the 1979 EAA. House versions of the EAA in the 107th Congress sought to explicitly define deemed export as exports falling under the jurisdiction of the act.”

15 See Report and Recommendation of the ABA Section on International Law regarding export controls. http://www.abanet.org/intlaw/regulation/export_rec.html. (Enforcing a requirement to obtain an export license to transfer technology within another country to a person located there when doing so does not affect the host country laws is a major offense to the sovereignty of the host country.).

were returned without action for additional information or were rejected (the reasons for rejection are not disclosed). The rejection rate now hovers at 1%.

Based on the foregoing figures, it appears that only a small fraction of license applications represent a risk. Moreover, it also appears that only a fraction of the entities that are subject to the current deemed export regime (based upon the technology they export and the individuals to whom they export it) currently understand the licensing requirement and submit deemed export license applications to BIS. This would appear to underscore the need (identified by the OIG but not addressed in the Notice) for enhanced education of the regulated community about the existing deemed export rule.

As there are no current data publicly available on whether any individuals having received deemed exports as authorized by license under the current regime have been found to have illicitly transferred technology in violation of the license conditions, the high license approval rate under the current regulations may indicate that the present regime is adequate to address the current problem, and that a more effective solution to illicit technology acquisition lies elsewhere.

Most important, the deemed export rule as it exists now is constitutionally suspect as an impermissible prior restraint on speech that violates the First Amendment to the Constitution. The proposal does not address this important point. First, the rule imposes broader curbs on speech than necessary to further the government's national security objectives. Some evidence of this is found in the pre-1994 rule, which was far narrower in scope but was not claimed to be too narrow to serve its purpose. Second, the procedures under the rule do not satisfy the prior restraint criteria: The restraint is not brief, judicial review is not expeditious (and indeed may be unavailable), and the burden of justifying the restraint is not placed upon the government entity imposing the restraint. The assertion of national security and foreign policy bases for restricting speech from one person in the United States to another have not been sufficient by themselves to overcome these constitutional restrictions. (New York Times Co. v. U.S., 403 U.S. 713 (1971). As recognized by the Ninth Circuit in Bernstein v. United States, the EAR’s export licensing system “allow[s] the government to restrain speech indefinitely with no clear criteria for review.” Bernstein v. United States, 176 F.3d 1132, 1145 (1999).

The deemed export rule is a poor tool to combat espionage, but it is not the only tool available to the BIS. The stated concern of the OIG in its report, and in its previous reports on deemed exports, has been that the deemed export rule needs to be somehow strengthened to prevent alleged transfers of sensitive U.S. technology abroad. Trying to use the deemed export licensing process to prevent this sort of industrial or economic espionage is inappropriate, since it is extremely unlikely that unauthorized transfers will be prevented through the licensing process. This is primarily because a person’s country of origin and employment history are poor predictors of their predilection to steal technology. The motive to steal and export dual-use trade and technology secrets can be predominantly financial, and U.S. citizens can be similarly motivated to steal sensitive U.S. technology and export it.
The EAR already contain better enforcement tools that are agnostic as to the nationality of the offender. General Prohibition 10 and EAR 764.2(e) prohibit releases of technology if the releasing party knows or has reason to know that it will be illegally exported, and similarly penalize any person – regardless of nationality, place of permanent residence, or place of birth - trying to steal and export technology abroad in violation of the EAR. Every one of the recent enforcement cases involving deemed exports could have been made by reference to violations of these provisions instead of the deemed export rule.

Similarly, prosecution of thefts of technology though the Economic Espionage Act and Trade Secrets laws present effective enforcement tools without imposing administrative burdens on companies seeking to employ foreign nationals. Given that the shortfall of qualified technical experts in software and high-tech industries is in the hundreds of thousands, the ability to effectively and efficiently hire foreign nationals to work in the high-tech sector is crucial to U.S. competitiveness.

The deemed export rule only came into being in 1994. The United States won the Cold War without a deemed export rule, and nobody has been able to demonstrate that the world is safer now because of the deemed export rule.

4. The Definition of “Use” Technology.

4.1 Proposed Change

The OIG report raises two linked issues relating to the definition of “use” technology in the EAR. The first issue concerns the use of the word “and” in the definition. Specifically in Section 772.1 of the EAR, the term “use” currently is defined as “Operation, installation (including on-site installation), maintenance (checking), repair, overhaul, and refurbishing.” The OIG expressed concern about the presence of the word “and” in the definition being interpreted to mean that all of the activities enumerated in the definition must be present in order to constitute “use.”

The OIG Report suggested that BIS revise the definition of “use” in Section 772.1 to replace the word “and” with the word “or,” as follows: “ ‘Use’ (All categories and General Technology Note)—Means all aspects of ‘use,’ such as: operation, installation (including on-site installation), maintenance (checking), repair, overhaul, or refurbishing.”

Separately, the OIG Report also recommends that guidance regarding the definition of “use” technology be revised to make it clear that the fundamental research exception to the deemed export rule does not apply to “use” technology for equipment used in conducting such research.

4.2 Comments
We do not foresee any problem with the proposed change from “and” to “or” in the wording of the definition of “use” technology, since the current form of the definition could reasonably be interpreted to be an illustrative list of activities constituting “use.” Any interpretation that required all of the items to be fulfilled would be strained, and is not likely to be used as a basis for contending under the current rule that an activity not fulfilling all elements is not considered “use” technology. A change from “and” to “or” in this provision does not raise concerns.

By contrast, however, we have serious concerns about second issue raised related to “use” technology. Specifically, the assumption inherent in the comment in the OIG Report is that mere access to EAR-controlled equipment by foreign nationals would necessarily constitute a deemed export of “use” technology. This is incorrect.

First, access to equipment is not prohibited by the deemed export rule. There is no deemed export rule for hardware or object code software, only for source code and technology. See 15 C.F.R. § 734.2(b)(2). Accordingly, any use technology gained from viewing and operating without instruction a product that can be viewed by the public is in the public domain, and thus not subject to the EAR under 15 C.F.R. Part 734. Second, most other “use” technology, such as published manuals for controlled machines, tends to be in the public domain (e.g., are freely available on the internet, available in a library, or available to any interested user through other prescribed channels), and thus not subject to the EAR under Part 734.

Even if some “use” technology is not in the public domain and is otherwise “subject to the EAR,” most technology categories in the EAR that are based on Wassenaar controls do not actually control “use” technology.

Even for those Export Control Classification Number (ECCN) categories where the EAR controls the “use” technology, the General Technology Note provides that technology is controlled only if it is “required” to achieve the relevant control parameter. 15 C.F.R. Part 774, Supp. No. 2. “Use” technology would rarely provide information regarding the technology of a piece of equipment required to achieve specific performance parameters – this is generally more typical of development and production technology.

Even to the extent that “use” technology is not in the public domain, and is controlled by an ECCN that would require a license to the home country of a foreign national, BIS policy since 1994 has been that License Exception TSU would authorize the export of the minimum necessary operations technology for the product.17 Again, there is no license

---

17 See Christensen, Technology and Software Controls under the Export Administration Regulations under the Export Administration Regulations, Practicing Law Institute, Coping with U.S. Export Controls 1999, 433, 454 (1999) citing six prior versions of the same article, each of which sat that “[o]ther License exceptions may also be used [for deemed exports] including the four different authorities of License Exception TSU.” Mr. Christensen wrote the original versions of these articles when he was Director of the Regulatory Policy Division of BIS. See also Flowe, Exporting Technology and Software, Particularly Encryption, Practicing Law Institute, Coping with U.S. Export Controls 2004, 249, 277 (2004) (describing applicability of TSU; author is a longstanding member of Regulations and Procedures Technical Advisory
requirement to provide a foreign national access to EAR-controlled equipment in the United States (i.e., no deemed export of hardware). Thus, basic operations and maintenance technology would be for “commodities or software that are lawfully exported or reexported under a license, a License Exception, or NRL [No License Required].” 15 C.F.R. § 740.13 (a). While it might be argued that TSU should not apply because there is no export or reexport upon which the TSU License Exception can rely, such an interpretation would make little sense. The logic and policy behind this TSU provision (which existed long before the deemed export rule) is that if the item can be accessed, the minimum necessary technology to operate the item should be accessible. That applies in the United States as well as outside the United States. To follow a more restrictive reading of this regulation would mean that, for example, if a license exception authorized export of the item to India, then related operations technology could accompany it and be received by Indian nationals there, while the same technology could not be given to an Indian national employed to operate the same machine in the United States. That type of logic would make the artificial deemed export rule a farce.

Moreover, in our experience, most companies have built compliance programs around the BIS long-standing policy that TSU would apply to deemed exports of basic operations technology, so have not attempted to classify technology related to basic operations and maintenance of equipment that employees use but do not design or develop. To do otherwise would be to create an administrative nightmare of work, that we believe in the end would still control virtually no technology.

As a result of the foregoing, it appears that the portion of the OIG Report focused on “use” technology is concerned with a level of technology rarely if ever controlled or worthy of attempting to control. In these circumstances, we respectfully recommend that any amended guidance regarding “use” technology clearly indicate that the deemed export rule only applies to such “use” technology that is both (a) subject to ECCN controls, and (b) required for the equipment to achieve controlled performance parameters. We also recommend that BIS make clear that License Exception TSU applies to the basic operation and maintenance technology even in those rare instances where “use” technology is controlled. We further recommend that any such amended guidance should not state or imply that such “use” technology is generally not subject to the “fundamental research” exemption.

5. Use of Foreign National’s Country of Birth as Criterion for Deemed Export License Requirement

5.1 Proposed Change

The OIG report expresses concern that current BIS deemed export license requirements are based on a foreign national’s most recent citizenship or permanent residency.
According to the OIG, this policy allows foreign nationals originally from countries of concern to obtain access to controlled dual-use technology without scrutiny if they maintain current citizenship or permanent resident status in a country to which the export of the technology would not require a license.

The OIG recommends that BIS amend its policy to require a deemed export license applications for foreign nationals who have access to dual-use controlled technology if they were born in a country where the technology export in question would require an export license, regardless of their most recent citizenship or permanent residency.

5.2 Comments

5.2.1. The OIG recommendation is not adequately supported by the OIG’s own analysis.

In reviewing the section of the OIG Report recommending a “country of birth” approach to deemed exports, we are not persuaded that the OIG recommendation is related to the analysis preceding it. This disjunction between analysis and recommendation may result in part from a lack of rigor in the application of terminology. For example, the header in the Report uses the term “nationalities.” Then in the first paragraph, the Report highlights the situation of individuals with “dual citizenship” and uses the terms “citizen,” “permanent residents,” “country of origin,” and “a person born in.” The OIG’s use of these terms is unclear and inconsistent, and the Report does not anywhere define what the OIG means by the term “country of origin.” Similarly, in the second paragraph the Report discusses “foreign nationals who originate” from countries of concern.” However, it is not clear what the OIG means by the term “originate.” Finally, the Report favorably cites the State Department’s policy to consider “all current nationalities,” and “dual citizenship” in addressing technical data exports.

While many of these terms have distinct legal meanings, it does not appear that the OIG was sensitive to their differences. For example, under the law of many countries, there is a distinction between nationals and citizens. In the United States, while expressions of “citizenship” and “nationality” are often used interchangeably, the term “citizen” is, as a rule, employed to designate persons endowed with full political and personal rights within the United States, while some persons – such as subjects of territories and possessions which are not among the states forming the Union – are described as “nationals.” “Nationals” owe allegiance to the United States, but do not possess full rights of citizenship in the United States. 18 From the statements made in the Report, it appears that the OIG intends for the BIS to adopt a policy in line with that of the Department of State, which is described as taking into account current dual citizenship status; however, the final OIG recommendation, which is based on “country of birth,” bears no relation to the Department of State, which is based on citizenship.

---

18 8 U.S.C. 1101(a)(22)
5.2.2. The proposal would undermine the role of nationality and nationality decisions in international law.

There are potential legal impediments and foreign policy repercussions to implementing the recommendations in the OIG Report. The nationality of an individual is his/her quality of being a subject of a certain state, and is a cornerstone of international law. Nationality has its origins in the notion of allegiance owed by the subject to his king, and traces of that underlying notion remain.\(^\text{19}\) Nationality is the basis for many fundamental principles of international law, including the right of a State to exercise diplomatic protection, or espousal, on behalf of its nationals and the right of a national to turn to his/her State for protection of his/her rights and property; and the obligation of a State to prevent and punish acts or omissions that violate the customary law of war and neutrality.\(^\text{20}\) While decisions regarding nationality are generally considered to be within the domestic jurisdiction of a State to determine who is, and who is not, its national\(^\text{21}\), States are required to adhere to standards of international law in making such determinations.\(^\text{22}\) As an example, it is not permissible for a state which has deprived a person of his/her nationality to reimpose its nationality upon that person against that person’s will, especially if he/she resides abroad.\(^\text{23}\)

Under international law, there is a duty to recognize foreign nationality determinations as long as they comport with these international standards.\(^\text{24}\) Moreover, under international law there is a presumption of the validity of naturalization status.\(^\text{25}\)

Because nationality and citizenship are so fundamental to international discourse, they form the basis of many treaties and conventions. To abandon these principles in favor of a rule based on “country of birth” would confound the paradigm of these agreements. For example, the Memorandum of Understanding (MOU) between the U.S. Joint Forces Command the Department of National Defense of Canada regarding liaison officers, which entered into force on January 31, 2003, outlines a framework for the exchange of military officers between the United States and Canada. This agreement contemplates the liaison officers having access to “classified” and “controlled unclassified information.” “Controlled unclassified information” includes information that is exempt from public disclosure or subject to export controls. Under the framework of this MOU, structures.


\(^\text{21}\) Jennings and Watts, at p. 852.

\(^\text{22}\) Id. at p. 389.

\(^\text{23}\) Jennings and Watts, at p. 83, f/n 8.


\(^\text{25}\) Brownlie at p. 403, citing the \textit{Nottebohm Case}, ICJ Reports (1955). (In that case, The International Court of Justice refused to recognize the nationality state’s right of diplomatic intervention when the bond between the individual and the state of nationality was too flimsy.)

30944494.2
the liaison officer is to be a national of the sending country. The sending country is to
give security assurances to the receiving country that its national will comply with all
reasonable security measures with respect to any information to which he or she has
access. Also under the MOU, information given to a liaison officer is to be considered
given to the government of that liaison officer, not to the government of his or her
“country of birth.” Identical or similar language exists in a number of other technical and
military cooperation agreements to which the United States is a party26.

The enactment of a deemed export rule based on country of birth would prevent the
United States from being able to fulfill its obligations under the framework of these
agreements. In the U.S.-Canada MOU example, in circumstances where the Canadian
representative is a national of Canada but was born in a different country, the U.S.
military would be prohibited under the proposed rule from providing access to controlled,
unclassified information under the agreement, despite the specific provision that such
access must be granted in order to fulfill the regime of the agreement. The same result
would be compelled under other technical and military cooperation agreements to which
the United States is a party. In our view, these implications have not been adequately
addressed, and may militate against the adoption of a deemed export regime based on
country of birth.

5.2.3 A survey of worldwide nationality laws indicates that country of
citizenship or permanent residence is a more reliable indicator of ties
to most countries than country of birth

Predicating the deemed export rule on a foreign national’s last acquired country of
citizenship or permanent residence (which is the standard under the current regime) is a
far more reliable and consistent indicator of one’s ties and allegiance to a country that the
often transitory circumstances of one’s birth.

We have reviewed the nationality laws of 184 countries worldwide. Of those only 43
generally confer citizenship on the basis of either the place of birth (“jus solis”) or by
descent through the nationality of one or more parent (“jus sanguinis”). Included in those
43 are, most notably, the United States, Cuba, France, Mexico, Brazil, and Canada.

The remaining 141 countries surveyed confer citizenship at birth, with minor exceptions,
exclusively by *jus sanguinis* (i.e., do not confer citizenship merely based on place of
birth). They include Iran, North Korea, Libya, Sudan, Russia, Vietnam, and the People’s

---

26 Separately, there may be issues of U.S. treaty obligations that should be addressed in connection with any
change in U.S. law that may affect principles of national treatment and most-favored-nation treatment.
Specifically, any treaty obligation that imposes national treatment with respect to engaging in commercial,
industrial, financial and other business activities within the territories of the other party may be implicated
by changes in U.S. policy regarding recognition of the nationality determinations of other countries as a
basis for being permitted to conduct business in the United States. For this reason, we recommend that any
consensus-building exercise with respect to the proposed rule should seek input from the United States
Trade Representative.
Republic of China, as well as Afghanistan, Austria, Belgium, Germany, Israel, Italy, Japan, the Netherlands, Pakistan, Spain, Taiwan, and the United Kingdom.

As an example, a child born in Iran would not be a citizen of Iran at birth unless one of the parents was born in Iran or the father was Iranian. However, under the OIG recommendation, a child born “in transit” through Iran to German parents, and thus not entitled to Iranian citizenship at birth under Iranian law, would nonetheless be considered “Iranian” for deemed export purposes. The same would hold true for the other 140 countries that apply the _jus sanguinis_ rule exclusively.

Even under the International Traffic in Arms Regulations (ITAR), birth in Iran, while a factor in the licensing determination, would not be conclusive in considering an application for a license for export of technical data. In the above example, the child, having no claim to Iranian citizenship, would be considered “German” rather than “Iranian” for ITAR licensing purposes.

**5.2.4 The process for acquiring permanent resident status and naturalization in third countries is generally comparable to U.S. standards, and in some cases is even more rigorous**

The OIG’s apparent concern that individuals could obtain a new “home country” through manipulation of lenient residency and naturalization processes of unsuspecting third countries appears unfounded, based on our review. While the rules for acquisition of permanent residency and naturalization in third countries vary, many countries have rigorous residence requirement and security reviews for both permanent residency and citizenship through naturalization.

A review of applicable permanent residency and naturalization requirements of Germany and Canada is particularly instructive. A significant number of Iranian citizens acquire interim German permanent residency or citizenship prior to seeking entry to the United States, while Canada is a significant destination for Chinese nationals. In both cases, the requirements and security standards for permanent residency and naturalization are comparable to U.S. standards.

Germany permanent residency, or _Niederlassungserlaubnis_, requires the applicant to have held a residence permit for at least five years. Applicants are subjected to a series of security and background checks that may take up to 6 months to complete. The requirements for naturalization are equally robust and require legal residence in Germany for eight years. With limited exception, naturalized German citizens are prohibited from holding dual citizenship, and must relinquish their previous citizenship as a condition of naturalization.

Permanent residence, or landed immigrant status, in Canada is based on categories for skilled workers, business immigrants (investors), or those with close family ties. These are similar to categories under the U.S. system, although the specific requirements and processes may differ. Naturalization under Canadian law requires residence in Canada
for at least three of the four years prior to application. Persons seeking permanent resident and naturalization under Canadian law are subject to extensive background screening for criminal activity as well as for potential ties to terrorism, and may be interviewed multiple times in order to satisfy Canadian immigration officials.

5.2.5. Foreign data protection regulations may hinder administration of and compliance with a regime based on country of birth

Several foreign jurisdictions have adopted strict rules on the collection, processing, and maintenance of personal data, including data on national origin. Examples of such regulations include the European Union (EU) General Data Protection Directive (“Directive”) and the EU Directive on Privacy and Electronic Communications. Entities collecting national origin data and other data may be required to obtain consent of the person whose data are collected, and the entities may be required to comply with regulations governing the accuracy, maintenance, and use of such data. Entities conducting certain activities with respect to personal data must be registered with the relevant EU and/or national governmental authority.

Beyond controlling the collection and maintenance of such data, the EU Directive also requires that the transfer of personal data to a third country (e.g., the United States) will only take place if the third country ensures “an adequate level of protection” for the data. The adequacy of such protection assessed in light of the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and the country of final destination, the rules of law in force in the third country, and the professional rules and security measures that are complied with in those countries. The EU does not consider U.S. law to provide an “adequate level of protection” for personal data. Accordingly, in order for data to be transferred from the EU to the United States, the entity transferring the data must comply with procedures established under the “Safe Harbor” process developed and administered by the U.S. Department of Commerce.

---


29 Many national jurisdictions have adopted regulations that are even stricter than those set forth in the EU directives. See, e.g., Germany—Federal Data Protection Act of the Federal Republic of Germany of December 20, 1990 (BGBI.I 1990 S. 2954), last amendment by law of May 23, 2001; Spain—The Organic Law on the Protection of Personal Data (Organic Law 15/1999 of 13 December); United Kingdom—The Data Protection Act of 1998 (Date of entry into force 1 March 2000, repealing the Data Protection Act 1984).

30 Directive, Article 25(1).

31 Directive, Article 25(2).
If the deemed export regime were revised to consider a foreign national’s country of birth, U.S. companies, universities, and other entities would be required to collect, transmit, and maintain national origin data concerning their employees, vendors, visitors, researchers, and other potential recipients of deemed exports. In cases where the persons whose data are being collected are within the jurisdiction of EU Directive or other foreign data privacy regulations, those laws may impose additional compliance burdens beyond those contemplated by BIS in the Notice.

6. Request for Clarification Through Additional Q&As

6.1 Proposed Changes

The OIG Report reviewed the effectiveness of BIS’ efforts to raise the awareness and understanding of the deemed export rule\textsuperscript{32}. The OIG recommended that BIS provide further guidance by clarifying and updating the EAR’s deemed export “Question and Answers” in Supplement No. 1 to Part 734\textsuperscript{33}. The OIG identified two examples of “Questions and Answers” that the OIG stated may be unclear or incorrect\textsuperscript{34}

6.2 Comments

We view the “Questions and Answers” format as beneficial, and we urge BIS to consider further revisions and modification to Supplement No. 1 to 15 C.F.R. Part 734.

Specifically, and germane to the substance of the OIG report, we suggest BIS publish additional “Questions and Answers” to address and clarify issues surrounding “use” technology. These might include, without limitation, the following:

**Question 1:** Does my company need a deemed export license to transfer controlled equipment to a foreign national in the U.S.?

**Answer 1:** The transfer of controlled equipment to a foreign national is not, in and of itself, a deemed export of controlled technology. However, if the visual inspection of that item transfers technology controlled by the EAR, then a deemed export license requirement may exist depending on the classification of the controlled equipment and the foreign national’s home country.

**Question 2:** A commercial retail establishment sells controlled manufacturing equipment, but maintains a unit of that equipment at its facility, housed in a glass case, and available for viewing during normal business hours by the general public.


\textsuperscript{33} Id., at 24.

\textsuperscript{34} Id., at 23.
My company purchased this equipment. Do we need to restrict foreign nationals from viewing the equipment?

**Answer 2:** If the sale of the equipment was open to all members of the public, then any technology that might be transferred during the viewing of the equipment is deemed to be publicly available under Part 734 of the EAR and, thus, not subject to the EAR.

**Question 3:** My company utilizes controlled equipment in the manufacturing process. The technology for the “use” of the equipment is controlled according to the General Technology Note. How does the General Technology Note impact our licensing analysis?

**Answer 3:** Under the General Technology note, only technology “required” for the use of an item is controlled\(^{35}\). “Required” is defined, in pertinent part, under EAR Part 772 as that “portion of ‘technology’ or ‘software’ which is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or function…”

Controlled performance levels are set forth in the ECCN definitions of the commodities for which technology is controlled. For example, if a commodity ECCN controls a widget which goes faster than X, then “required” technology would be limited to that which is responsible for the widget to achieve or exceed that speed.

On the other hand, if the controlled equipment is contained within a black box, the casual observation of the box would not convey “use” technology that is peculiar, or required, to operate the controlled equipment. [We would note that if BIS decides to change the word “and” to “or” in its definition of use technology, paragraph 2 of this answer would read, in relevant part, “peculiarly responsible for the operation, installation, maintenance, repair, overhaul or the refurbishing of controlled equipment”].

7. **Conclusion**

We thank BIS and the Department of Commerce for the opportunity to provide these comments, which we hope will be helpful. Should you have any questions regarding these comments, please feel free to contact me, or J. Scott Maberry, Chair of our Export Controls and Economic Sanctions Committee, at (202) 662-4693, or by e-mail at smaberry@fulbright.com.

Sincerely,

Kenneth B. Reisenfeld,
Chair

\(^{35}\) 15 C.F.R. 774, Supp. No. 2.
CC:

J. Scott Maberry  
Chair, Committee on Export Controls and Economic Sanctions  
American Bar Association  
Section on International Law

U.S. Department of Commerce, via Federal e-Rulemaking Portal:  

U.S. Department of Commerce, via e-mail: scook@bis.doc.gov (Subject: “RIN 0694-AD29”)