

8-1-1984

## The Current Legal Basis for Controls on the “Export” of Technical Information

Americo R. Cinquegrana

John Michael Shepherd

Follow this and additional works at: <http://lawdigitalcommons.bc.edu/iclr>

 Part of the [Science and Technology Commons](#)

---

### Recommended Citation

Americo R. Cinquegrana and John Michael Shepherd, *The Current Legal Basis for Controls on the “Export” of Technical Information*, 7 B.C. Int'l & Comp. L. Rev. 285 (1984), <http://lawdigitalcommons.bc.edu/iclr/vol7/iss2/5>

This Article is brought to you for free and open access by the Law Journals at Digital Commons @ Boston College Law School. It has been accepted for inclusion in Boston College International and Comparative Law Review by an authorized administrator of Digital Commons @ Boston College Law School. For more information, please contact [nick.szydowski@bc.edu](mailto:nick.szydowski@bc.edu).

# The Current Legal Basis for Controls on the “Export” of Technical Information†

by *Americo R. Cinquegrana\**  
and *John Michael Shepherd\*\**

## I. INTRODUCTION

In the last several years, considerable public and government attention has been directed to the acquisition of Western strategic technology by potential military adversaries of the United States, particularly the Soviet Union.<sup>1</sup> Confronted by the Eastern bloc's overwhelming superiority in manpower and sheer volume of weaponry, Western security is dependent on advanced technology. Congressional studies and intelligence reports have identified a significant Soviet effort to satisfy the immediate demands of its military structure.<sup>2</sup> As Senator William Roth has declared:

There is no question that the Soviets have undertaken a massive, well-financed, expertly coordinated program to systematically acquire as much [of] our high technology as they can steal, purchase through middlemen or otherwise appropriate. And all because they are unable to produce that technology themselves. So they are left to copy ours and use it, [not] to make life more comfortable for their citizens, but to advance their numerous weapons systems and overall military capabilities.<sup>3</sup>

The primary emphasis of the Western response to this threat is on the control of exports of goods. As enforcement efforts are increased and improved, further study has been given to the extent to which the acquisition of technical informa-

---

† The analysis and conclusions included in this article are those of the authors and do not necessarily represent the official views of the Department of Justice.

\* Deputy Counsel to the Attorney General for Intelligence Policy, U.S. Department of Justice.

\*\* Special Assistant to the Assistant Attorney General, Office of Legal Policy, U.S. Department of Justice.

1. See, e.g., *Transfer of United States High Technology to the Soviet Union and Soviet Bloc Nations: Hearings Before the Permanent Subcomm. on Investigations of the Senate Comm. on Governmental Affairs*, 97th Cong., 2d Sess. 193-216 (1982) (statement of William von Raab, Commissioner, U.S. Customs Service Regarding Operation EXODUS) [hereinafter cited as *Senate Hearings*].

2. See SENATE COMM. ON GOVERNMENTAL AFFAIRS, REPORT ON TRANSFER OF UNITED STATES HIGH TECHNOLOGY TO THE SOVIET UNION AND SOVIET BLOC NATIONS, S. REP. NO. 664, 97th Cong., 2d Sess. 32 (1982).

3. *Id.* at 1.

tion contributes to the diminution of the West's technological lead.<sup>4</sup> Knowledgeable parties have urged that control mechanisms should be focused on technological "know-how" and manufacturing information, as opposed to end-products, since the adaptation and application of such information will have the most enduring impact on military and industrial capabilities.<sup>5</sup> Others, while not disagreeing with that assessment, counsel caution in devising controls on information which may exceed the scope of the problem and have the unintended and undesirable effect of constraining scientific and academic communication and impeding our own technological advancement.<sup>6</sup>

This paper provides brief, essentially nontechnical, summaries of the legal mechanisms which authorize the U.S. government to control the communication of technical information that might improve the military capabilities of its potential adversaries.<sup>7</sup>

## II. SCOPE AND DEFINITIONS

Existing laws and regulations provide authority for government control of technical information that is under the control of the government or that is in private hands and has certain identifiable applications. These laws and regulations do not provide the government with general authority to control privately developed technical information that appears to have no practical military or industrial value.

Given the high rate of technological advancement in the private sector, technical information of no apparent practical application today may be the basis for a revolutionary breakthrough (usually identified as an "emerging technology") in the near future.<sup>8</sup> Nonetheless, it would be nearly impossible, as has been acknowledged impliedly in the current control structure, to attempt to control all information that has uncertain practical value. Accordingly, this discussion

---

4. See, e.g., *id.* at 235-49 (testimony of Adm. Bobby R. Inman, Deputy Director of Central Intelligence); see also, COMMITTEE ON SCIENCE, ENGINEERING AND PUBLIC POLICY, NATIONAL ACADEMY OF SCIENCES, SCIENTIFIC COMMUNICATION AND NATIONAL SECURITY, (1982) (Report of the Panel on Scientific Communication and National Security) [hereinafter cited as SCIENTIFIC COMMUNICATION AND NATIONAL SECURITY].

5. See, e.g., Final Report of the Defense Science Board Task Force on Export of U.S. Technology, February 1976.

6. *Id.*; see also SCIENTIFIC COMMUNICATION AND NATIONAL SECURITY, *supra* note 4; T. GUSTAFSON, SELLING THE RUSSIANS THE ROPE? SOVIET TECHNOLOGY POLICY AND U.S. EXPORT CONTROLS (1981) (Rand Corp. Study for the Defense, Advanced Research Projects Agency, Santa Monica, CA).

7. This paper does not address technical information that may be classified as national security information under Exec. Order No. 12,356, 47 Fed. Reg. 14,874 (1982). Rather, it assumes that technical information produced by or for the U.S. government that may and should be classified will be identified and controlled on that basis. The subject of this paper is technical information that the government has not classified or that is not in the possession or control of the U.S. government and, therefore, cannot be classified.

8. See *Senate Hearings, supra* note 1, at 262-77 (testimony of Lawrence J. Brady, Assistant Secretary for Trade Administration, U.S. Department of Commerce).

focuses on what we have called "development information," as differentiated from "research information" that exists primarily to foster further study.

"Research information," for purposes of this paper, is defined as the product of systematic study and experimentation intended to improve understanding of fundamental phenomena. Such information is not developed for specific commercial or military uses, but is pursued primarily to increase human knowledge. The process by which such information is produced is often referred to as "basic" or "fundamental" research. "Development information" is defined for purposes of this paper as the product of systematic design, fabrication, or experimental efforts to translate an application concept into specifications, models, or design data necessary for the effective production of a product or the effective use of a process. This category of information is generically identified as "technical data" in the most important current control mechanisms.<sup>9</sup>

In addition to defining the basic types of information that are discussed here, it is necessary also to define several terms that are used to determine when information that is otherwise within the scope of the control mechanisms will not be subject to further controls because of its widespread availability. Information is "published" when it is made available in tangible form to any person through purchase, free distribution, or public libraries. Mere submission to a publisher or editor does not, however, constitute publication.<sup>10</sup> Information is "publicly available" in the context of this paper when it has been published, approved for public release by the department or agency that has responsibility for the information, or disclosed at a conference, trade show, or other meeting that is open to the public.<sup>11</sup> "Open to the public," as used here, means the event may be attended by technically qualified members of the public (subject only to administrative considerations such as space limitations and payment of registration fees) and it is expected that conference proceedings, reports, or the like will be published in the reasonably foreseeable future.<sup>12</sup>

### III. SOURCES OF AUTHORITY FOR CONTROL OF TECHNICAL INFORMATION

The three primary sources of authority for U.S. government controls over the communication of "development information" are: (a) the Export Administration

---

9. Export Administration Regulations, 15 C.F.R. § 379.1(a) (1983); International Traffic In Arms Regulations, 22 C.F.R. § 125.01 (1983). As is explained later in this paper, these regulations identify the technical information that is subject to government controls by its setting on the continuum between pure research and full-scale production. Although necessary in practice, this approach presents a fundamental dilemma since the conceptual basis for controlling the export of the information is not the context in which it appears but the nature of the information and its perceived value.

10. Cf. Export Administration Regulations, 15 C.F.R. § 379.3(a) (1983) (for definition of "Data Generally Available").

11. Cf. *id.*; 22 C.F.R. §§ 125.11-12 (1983). See *infra* text accompanying notes 44-45.

12. *Id.*

Act of 1979,<sup>13</sup> and its implementing regulations,<sup>14</sup> for information having both civilian and military applications; (b) the Arms Export Control Act,<sup>15</sup> and its implementing regulations,<sup>16</sup> for information pertaining solely to defense articles and defense services; and (c) the Atomic Energy Act,<sup>17</sup> for information relating to nuclear materials, weapons, and applications.

Other sources of authority are applicable in particular circumstances. The Invention Secrecy Act of 1951 and its regulations<sup>18</sup> may be the basis for a secrecy order in instances where technical information contained in a patent application requires controls for national security purposes. Additional sources of specialized authority include the Trading With the Enemy Act and its regulations<sup>19</sup> and the International Emergency Economic Powers Act (IEEPA).<sup>20</sup> The former statute is applicable generally in commercial dealings with specific, previously designated foreign countries, while the latter statute requires a declaration of national emergency for its invocation.<sup>21</sup>

The Export Administration Act and the Arms Export Control Act are applied at present through their implementing regulations to cover only "development information" rather than "research information."<sup>22</sup> The Atomic Energy Act applies not only to development information that relates to atomic energy and nuclear materials, but also to research information, since such information is of manifest practical value.<sup>23</sup> The Trading With the Enemy Act and the International Emergency Economic Powers Act also may apply to both types of information when they appear in a commercial context.<sup>24</sup> The Invention Secrecy Act, by its nature, contemplates practical application since it applies to information included in a patent application.<sup>25</sup>

13. 50 U.S.C. app. §§ 2401-2420 (1982 & Supp. I 1983).

14. 15 C.F.R. §§ 368.1-399.1 (1983).

15. 22 U.S.C. §§ 2751-2794 (1982).

16. 22 C.F.R. §§ 121.01-130.33 (1983).

17. 42 U.S.C. §§ 2011-2296 (1982).

18. 35 U.S.C. §§ 181-188 (1982); 37 C.F.R. §§ 5.1-.23 (1983).

19. 50 U.S.C. app. §§ 1-44 (1982 & Supp. I 1983); 31 C.F.R. § 500.101-520.809 (1983).

20. 50 U.S.C. §§ 1701-1706 (Supp. 1983) (IEEPA).

21. The IEEPA was invoked in a variety of contexts to deal with the Iranian hostage crisis. Exec. Order Nos. 12,170, 44 Fed. Reg. 65,729 (1979); 12,205, 45 Fed. Reg. 24,099 (1980); 12,211, 45 Fed. Reg. 26,685 (1980); 12,276-12,284, 46 Fed. Reg. 7,913-31 (1981); 12,307, 46 Fed. Reg. 30,483 (1981); 12,317, 46 Fed. Reg. 42,241 (1981); 12,379, 47 Fed. Reg. 36,100 (1982). More recently, IEEPA has been invoked in Exec. Order No. 12,444, 48 Fed. Reg. 48,215 (1983), which extended the Export Administration Regulations for several weeks between the expiration of the Export Administration Act and its extension by Congress through February, 1984, and again in Exec. Order No. 12,470, 49 Fed. Reg. 13,099 (1984) when the congressional extension expired.

22. See *supra* note 9.

23. See *supra* note 17.

24. See *supra* notes 19 and 20.

25. See *supra* note 18.

A. *Export Administration Act and Export Administration Regulations*

The Export Administration Act (EAA),<sup>26</sup> which is administered by the Commerce Department,<sup>27</sup> encompasses a broad range of "development information," identified in this context as "technology" or "technical data."<sup>28</sup> The statutory language demonstrates that Congress contemplated export controls of certain types of information as well as hardware and equipment, since the statute refers repeatedly to control of both "goods [and/or] technology,"<sup>29</sup> and "technology" is defined to include a variety of information of practical value, including technical data.<sup>30</sup>

The Secretary of Commerce maintains the Commodity Control List (CCL) which identifies the "goods" and "technology" that are subject to the licensing requirements of the EAA.<sup>31</sup> The "technology" that is subject to EAA controls is defined in the Export Administration Regulations (EAR) as technical data "that can be used, or adapted for use, in the design, production, manufacture, utilization, or reconstruction of articles or materials" without reference to whether those articles or materials are themselves included on the CCL.<sup>32</sup> This information may be in tangible form, such as blueprints or manuals, or may be conveyed by intangible means, such as by the provision of technical services.<sup>33</sup>

The 1979 revision of the EAA required the Defense Department to develop a list of technologies considered to be militarily "critical."<sup>34</sup> This list was to be prepared for incorporation in the Commodity Control List, thereby facilitating control of these "militarily critical" technologies.<sup>35</sup> This process has not been completed to date, although DOD has published a "Table of Contents" for the list.<sup>36</sup>

The EAA authorizes export controls for three basic purposes: (a) to protect U.S. national security interests, (b) to further U.S. foreign policy objectives, and (c) to protect the U.S. economy by limiting the export of materials that are in short supply domestically.<sup>37</sup> The national security controls are the most important of the three for purposes of this discussion, since they may be applied to any transfer of technology that would make a significant contribution to the military

---

26. See 50 U.S.C. app. § 2415(4) (1982 & Supp. I 1983).

27. 50 U.S.C. app. §§ 2409, 2411, 2415(5) (1982 & Supp. I 1983).

28. 15 C.F.R. § 379.1(a) (1983).

29. See, e.g., 50 U.S.C. app. §§ 2401(5), 2401(8), 2402(2), 2402(6) (1982 & Supp. I 1983).

30. 50 U.S.C. app. § 2415(4) (1982 & Supp. I 1983).

31. *Id.* § 2403(b) (1982 & Supp. I 1983).

32. 15 C.F.R. § 379.1(a) (1983).

33. *Id.*

34. 50 U.S.C. app. § 2404(d)(2) (1982 & Supp. I 1983).

35. *Id.* § 2404(d)(3)-(d)(5) (1982 & Supp. I 1983).

36. 45 Fed. Reg. 65,014 (1980). The Department of Energy also published a "List of Energy Related Militarily Critical Technologies" in support of the DOD effort. 45 Fed. Reg. 65,152 (1980).

37. 50 U.S.C. app. § 2402(2) (1982 & Supp. I 1983).

potential of any country that would be detrimental to the national security of the United States.<sup>38</sup> The Export Administration Regulations extend this authority to any person or technology within the jurisdiction of the United States<sup>39</sup> and restrict exports of technical data from the United States, reexports of U.S.-originated technical data from one foreign destination to another, and exports or reexports between foreign destinations of foreign materials that incorporate U.S.-originated technical data.<sup>40</sup>

Any transfer of "development information" that falls within these broad controls over technical data requires a validated, i.e., specifically approved license, except to the extent that the EAR provide a general license, i.e., no specific approval required for transfers of publicly available, scientific or educational data, or for transfers to certain destinations.<sup>41</sup> Since the EAR controls of technical data are broader than those concerning goods, there may be circumstances where a license would be required for the export of "development information" even though no license would be required for the export of goods produced by that technology. This conclusion is based on the fact that technology relating to nonmilitary commodities that are uncontrolled may be useful for the production of military materials.

"Export" is defined in the EAR to include not only any actual transmission of "development information" out of the United States, but also any release of such information in the United States with knowledge or intent that the information will be transmitted out of the United States or any release abroad of such information that originated in the United States.<sup>42</sup> Such release of information may take the form of visual inspection of equipment or facilities by foreign nationals, oral exchanges in the United States or abroad, or the application abroad of knowledge or experience acquired in the United States.<sup>43</sup>

A broad definition of "technical data" thus is combined with a broad definition of "export" to require, with very few exceptions, a license for virtually any disclosures to foreign nationals in the United States or any transmission or use abroad of most "development information." As mentioned, the EAA and EAR contemplate two basic types of licenses: "general" and "validated." The broad authority asserted by the expansive definitions in the EAR is made less burdensome through the creation of general licenses. These licenses have the character of regulatory exemptions and generally require no formal application or notice

38. *Id.* § 2402(A).

39. The jurisdiction of the United States may reach persons and information outside the United States, its possessions, and territories. *See id.* §§ 2404(a), 2415(2); 15 C.F.R. §§ 379.1(b), 379.1(c), 379.8 (1983).

40. 15 C.F.R. §§ 379.1(b), 379.1(c) (1983).

41. *Id.* §§ 370.3(a), 379.2-379.6.

42. *Id.* § 379.1(b)(1).

43. *Id.* § 379(b)(2).

to the Department of Commerce, so long as the export of the technical data in question meets the standards articulated in the EAR.

One type of general license permits any export of "development information"<sup>44</sup> that has been made generally available to the public in any form. This concept of public availability includes oral or visual release at "open" conferences, lectures, trade shows, and in publications that are free or available without restriction for the cost of publication rather than the commercial value of the data or are readily available at libraries open to the public.<sup>45</sup> While there is little administrative guidance available on the subject, an "open" conference could be characterized as one that features advance announcement or other notice that indicates the session is known and may be attended by any technically qualified members of the public, subject to administrative considerations such as space limitations and the payment of registration fees, and an intent that proceedings, reports, or the like will be published and readily available in connection with the conference.

A general license also permits release of scientific or educational information that is not directly and significantly related to the design, production, or utilization of industrial processes: "research information."<sup>46</sup> Authority is also provided for academic classroom or laboratory instruction involving such information so long as the subject is not contract research directly and significantly related to industrial purposes or processes: "development information."<sup>47</sup> Limited general license authority is also available in certain situations involving U.S. or foreign patent applications.<sup>48</sup>

The second type of general license that is provided in the EAR for the transfer of "development information" is more limited and depends on the nature of the information and its intended destination.<sup>49</sup> Generally, the export of such information relating to nonmilitary industrial processes to Free World countries is permitted, although in some cases the recipient must provide written assurance that the data will not be reexported.<sup>50</sup> This license is not available where there is reason to believe the data is related to certain identified products or processes.<sup>51</sup>

Except for transfers to Canada, where most types of information may be sent without a license of any type,<sup>52</sup> any transfer of "development information" that is directly related to an item on the Commodity Control List, or is directly and significantly related to any industrial process, requires a validated license for

---

44. *Id.* § 379.3(a).

45. *Id.*

46. *Id.* § 379.3(b)(1).

47. *Id.* § 379.3(b)(2).

48. *Id.* § 379.3(c).

49. *Id.* § 379.4.

50. *Id.* § 379.8.

51. *Id.* § 379.4(c).

52. *Id.* § 379.2, n.7.



export to countries to which exports are controlled for national security purposes.<sup>53</sup> Such licenses require the approval of the Department of Commerce.<sup>54</sup> Where the information in question has been developed in whole or in part as a direct or indirect result of Department of Defense funding, the approval of the Department of Defense may also be necessary.<sup>55</sup>

As noted above, information of whatever nature, whether "research" or "development," is not subject to the EAA and EAR formal validated licensing requirements if it has been made "publicly available."<sup>56</sup> This means that the information has been made available in the public media, is available at public libraries, or is available for merely the cost of its publication rather than its intrinsic value.<sup>57</sup> The EAR apparently presumes that the owners of commercially valuable information will, in effect, identify the information requiring license approval for its transfer by their efforts to protect it.

#### B. *Arms Export Control Act and International Traffic in Arms Regulations*

The Arms Export Control Act (AECA)<sup>58</sup> provides the legal authority to control the transfer of articles and services that have direct military application. While the statute does not provide expressly that "information," such as "technical data" as defined in the EAR, is included within the meaning of the terms "defense services" or "defense articles," the language of the act is sufficiently broad to authorize controls over this area.<sup>59</sup> This authority, administered by the Department of State, is implemented by the International Traffic In Arms Regulations (ITAR).<sup>60</sup> Those articles and services for which a license is required prior to exportation are designated in the ITAR's U.S. Munitions List, by the Secretary of State with the concurrence of the Secretary of Defense.<sup>61</sup>

Unlike the EAA and EAR controls, which differ depending upon the particular destination to which the controlled technology is being exported, the AECA and ITAR control the export of defense-related materials and technical data, as well as classified information, to all foreign destinations. All exports of such items to certain countries are prohibited as a matter of national security policy.<sup>62</sup>

The U.S. Munitions List, like the Commodity Control List, controls "technical

53. *Id.* § 379.5(a).

54. *Id.*

55. *Id.* §§ 370.10, 379.1(b) n.4.

56. *Id.* § 379.3(a).

57. *Id.*

58. 22 U.S.C. §§ 2751-2794 (1982).

59. *Id.* §§ 2403(e), 2778, 2794(4) & (7).

60. 22 C.F.R. §§ 121.01-122.22 (1983).

61. 22 U.S.C. § 2778 (1982); Exec. Order No. 11,958, § 1(e), 42 Fed. Reg. 4311 (1977), as amended by Exec. Order No. 12,118, 44 Fed. Reg. 7939 (1979).

62. 22 C.F.R. §§ 123.01, 123.10, 126.01 (1983).

data" related to items on the list.<sup>63</sup> Although slightly different from the definition in the EAR, the ITAR definition of "technical data" is equally broad. Generally, the ITAR definition also applies to "development" rather than "research" information. The definition includes classified information relating to items on the U.S. Munitions List, but also:

[a]ny unclassified information that can be used, or be adapted for use, in the design, production, manufacture, repair, overhaul, processing, engineering, development, operation, maintenance, or reconstruction of arms, ammunition, and implements of war on the U.S. Munitions List; or (b) any technology which advances the state-of-the-art or establishes a new art in an area of significant military applicability in the United States; . . .<sup>64</sup>

With respect to subpart (b) of this definition, the exporter has the specific duty to consult with appropriate U.S. government officials and to determine whether the technical data in question "advances the state-of-the-art or establishes a new art."<sup>65</sup>

These provisions may be applicable to "research information" or "emerging technologies" if "state-of-the-art" is intended to include any new information in any area that may have military significance. The reference in subpart (b) of the definition to "significant military applicability," however, seems to imply practical use and may serve to exclude information that is not "development information."

The ITAR controls on technical data apply whether the information is disclosed orally, visually, or by documentary means.<sup>66</sup> The regulations apply whether the information in question is transmitted out of the United States by human or other means, whether the "export" occurs in the course of visits or participation in conferences and trade fairs abroad by U.S. citizens, or by visits or participation in conferences and trade fairs in the United States by foreign nationals.<sup>67</sup>

As with the EAA and EAR, regulatory exemptions narrow the expansive reach of these ITAR provisions. Under the ITAR, however, the format of the exemptions is to require no license in certain circumstances, rather than to create a general license requiring no formal application or review.<sup>68</sup> Several limited exemptions may be relevant in particular situations. For example, most unclassified information may be exported to Canada,<sup>69</sup> and no license is required to ship additional copies of information previously exported to the same recipient

---

63. *Id.* § 121.01, *id.* § 125.01-125.24.

64. *Id.* § 125.01(a) (1983) (emphasis added).

65. *Id.* § 125.01 n.1.

66. *Id.* § 125.03.

67. *Id.* §§ 125.03, 125.04(c).

68. *Id.* §§ 125.11, 125.12.

69. *Id.* § 125.12.

under a license.<sup>70</sup> An important exemption provides that no license is necessary for the export of "technical data" that is "in published form and subject to public dissemination."<sup>71</sup> This exemption includes information that is: "(a) sold at newsstands and bookstores; (b) available without charge or by subscription or purchase to any person without further restriction; (c) determined to be eligible for second-class mailing privileges; or (d) freely available at public libraries."<sup>72</sup>

As under the EAR, these provisions apparently embody an assumption that persons or entities in possession of information will act in their commercial self-interest to identify that information which is valuable and worthy of protection. Unlike the EAR, however, the ITAR provide that persons seeking to publish "technical data," whether or not developed under contract with the government, have the burden of obtaining appropriate U.S. government approval.<sup>73</sup> This ITAR requirement seems to require an export license in order to publish "development information" in the United States. To the best of our knowledge, however, it has never been applied to prevent publication of such information<sup>74</sup> and has not been tested in the courts. The general prohibition in the ITAR on exporting technical data has been upheld, however, as to information directly and significantly related to specific articles on the Munitions List.<sup>75</sup>

The ITAR require prior State Department approval for presentations to foreigners that involve information concerning Munitions List items and the disclosure of technical data.<sup>76</sup> Further, the ITAR require that manufacturing or technical assistance agreements between persons in the United States and persons abroad relating to items on the Munitions List be approved by the Department of State<sup>77</sup> and include certain conditions, such as a bar on disclosure of technical data to particular third countries.<sup>78</sup> Thus, the ITAR control the exportation of "development information" under manufacturing licenses or technical assistance agreements when that information relates to items on the Munitions List or a new area of significant military capability.

The AECA licensing process for the export of technical data has two main elements. First, the sensitivity of the data is evaluated by the State Department and the appropriate elements of the Defense Department, as well as other agencies when necessary because of the nature of the data involved.<sup>79</sup> Second, State reviews the proposal for consistency with U.S. foreign policy objectives.<sup>80</sup>

---

70. *Id.* § 125.11(8).

71. *Id.* § 125.11(1).

72. *Id.*

73. *Id.* § 125.11(1) n.3.

74. See *infra* note 86 and accompanying text.

75. See *United States v. Edler Industries*, 579 F.2d 516 (9th Cir. 1978).

76. 22 C.F.R. § 125.03 (1983).

77. *Id.* § 124.01.

78. *Id.* § 124.10(i).

79. *Id.* §§ 124.02, 125.05.

80. *Id.* §§ 123.05, 124.01.

Unlike the EAA process, no specific reference is made to the foreign availability of the information in question. This factor would not be determinative in a licensing decision under the AECA except to the extent that such availability has an obvious bearing on the sensitivity of the export.

The authority of the Department of Commerce to impose export controls under the EAA extends only to items not controlled by other statutes.<sup>81</sup> Where it is unclear whether the EAA or the AECA applies, Congress has directed the Commerce Department to coordinate the application of the EAA with the AECA.<sup>82</sup> Thus, there may be cases where Commerce will require the approval of the State Department before granting an export license.

The State Department issued a policy statement in 1980 that was intended to clarify the scope of the ITAR controls on "technical data" in the context of cryptography.<sup>83</sup> Technical data was described as not including general mathematical, engineering, statistical, or other basic and theoretical ("research") information that is not reasonably expected to have direct application to items on the Munitions List (i.e., "development information").<sup>84</sup> The statement also reaffirmed that professional and academic presentations, informal discussions, and equipment demonstrations that involve disclosure of "technical data" to foreign nationals require State Department approval.<sup>85</sup> The policy statement also advised, however, that no prior approval is required for publication of information in the United States, within the meaning of the ITAR provisions authorizing a general exemption from the AECA licensing requirement, for information "in published form and subject to public dissemination."<sup>86</sup> Those provisions were not intended, despite the explicit reference to obtaining "appropriate" U.S. government approval before publication, to establish a prior review requirement.<sup>87</sup>

### C. Atomic Energy Act

Under the terms of the Atomic Energy Act,<sup>88</sup> all information, whether "research" or "development" in nature, that concerns the design, manufacture or use of atomic weapons, the production of special material, or the use of such material in energy production is designated as "restricted data" and therefore

---

81. 50 U.S.C. app. § 2416(a) (1982 & Supp. I 1983); 15 C.F.R. § 370.10(a) (defense materials) and § 370.10(e) (nuclear materials) (1983).

82. 50 U.S.C. app. § 2416(b) (1982 & Supp. I 1983).

83. *Cryptography/Technology Data*, 80 DEP'T OF STATE MUNITIONS CONTROL NEWSLETTER (1980).

84. *Id.*

85. *Id.*

86. *Id.*; 22 C.F.R. § 125.11(1) (1983).

87. *Cryptography/Technology Data*, 80 DEP'T OF STATE MUNITIONS CONTROL NEWSLETTER (1980); 22 C.F.R. § 125.11(1) n.3 (1983).

88. 42 U.S.C. §§ 2011-2296 (1982).

subject to the control of the Department of Energy, successor to the Atomic Energy Commission for these purposes.<sup>89</sup> Information within the restricted data category is "born classified" in that it is subject to government control as restricted data from the moment of its development, even when the information has been developed entirely in the private sector.

This broad assertion of government control over the disclosure and use of this particular category of information has been challenged and sustained in the courts. In *United States v. The Progressive*,<sup>90</sup> the government obtained a preliminary injunction, which withstood subsequent review,<sup>91</sup> against the publication of information concerning the construction of a hydrogen bomb. The cases were ultimately dismissed, at the request of the government, because similar information published elsewhere had been widely disseminated.

The act establishes specific controls and requirements for the export of restricted data.<sup>92</sup> Such information may only be exported pursuant to a special agreement for nuclear cooperation authorized by the President.<sup>93</sup> The act also establishes penalties for illegal acts involving restricted data.<sup>94</sup> Information that has been declassified or removed from the restricted data category may be controlled under a 1982 addition to the Atomic Energy Act.<sup>95</sup> Proposed Department of Energy regulations were published to establish these controls in April, 1983. Other information related to the security of nuclear facilities may be controlled by the Nuclear Regulatory Commission and the Department of Energy under provisions enacted in 1980 and 1982, respectively.<sup>96</sup>

Unclassified information relating to the production of special nuclear material abroad, not authorized under an agreement for cooperation with a foreign country, may not be transferred to that country without authorization by the Department of Energy.<sup>97</sup> Authorization by the Department of Energy does not preclude the Commerce Department from requiring a validated license for the export of "technical data" under the Export Administration Act.<sup>98</sup> Finally, the Atomic Energy Act establishes rigorous export controls over the export of information defined to be "sensitive nuclear technology" in the Nuclear Non-Proliferation Act of 1978.<sup>99</sup>

Thus, control may be asserted under the Atomic Energy Act over the publica-

89. *Id.* § 2014(y).

90. 467 F. Supp. 990 (W.D. Wis. 1979).

91. *Motion for reconsideration denied*, 486 F. Supp. 5 (W.D. Wis. 1979); *appeal dismissed without opinion*, 610 F.2d 819 (7th Cir. 1979).

92. 42 U.S.C. §§ 2162, 2164 (1982).

93. *Id.*

94. *Id.* §§ 2272-2277 (1982 & Supp. I 1983).

95. *Id.* § 2168 (1982 & Supp. I 1983).

96. *Id.* §§ 2167, 2168 (1982 & Supp. I 1983).

97. *Id.* §§ 2131-2140 (1982).

98. *Id.* § 2166 (1982).

99. 22 U.S.C. §§ 3201-3282 (1982).

tion or "export" of either "research" or "development" information that constitutes restricted data. The Nuclear Regulatory Commission has the authority to review, declassify, and remove information from this category when it determines that publication would not constitute "an unreasonable risk to the common defense and security," although in some instances the concurrence of the Department of Defense is required.<sup>100</sup>

#### D. *Invention Secrecy Act*

The Invention Secrecy Act of 1951 (ISA)<sup>101</sup> authorizes the government to prevent the public dissemination, through the patent system, of information submitted in connection with an application for patent protection. This control is accomplished by the issuance of a secrecy order precluding the applicant from disclosing further the information in the application.<sup>102</sup> The authority first was enacted in 1917 and was limited to time of war in both its effect and duration. In 1940, the wartime limitation was removed and the Commissioner of Patents was empowered to withhold the award of a patent for any period determined to be in the national interest. This authority was extended for the duration of World War II in 1942, and was made permanent in 1952.

Information included in a patent application is kept in confidence by the Patent Office and is not disclosed until a patent is granted. A small staff in the Patent Office performs a national security review of each of the approximately 100,000 patent applications that are filed each year. This staff is allotted six months for its review and for any necessary consultation with and review by the defense agencies.<sup>103</sup> The staff relies for guidance in its review on the Commodity Control List, the Munitions Control List, and the Militarily Critical Technologies List, as well as general information acquired in the course of its dealings with the various national security and export control agencies. During the review period, the applicant may not seek a foreign patent for an invention made in the United States without a "license" from the Patent Office.<sup>104</sup>

The ISA does not bar publication of information by an applicant prior to filing a patent application, however, and a patent may be granted after publication so long as the application was filed prior to, or within one year of the publication date.<sup>105</sup> This situation obviously would negate the effectiveness of any secrecy order and, again, demonstrates an underlying reliance on the commercial self-interests of the possessor of the relevant information.

---

100. 42 U.S.C. § 2162(b) (1982).

101. 35 U.S.C. §§ 181-188 (1982).

102. *Id.* § 181.

103. *See* Rules of Practice In The Patent Office, 37 C.F.R. §§ 5.1-23 (1983).

104. 35 U.S.C. § 184 (1982).

105. *Id.* § 119.

The ISA establishes two categories of authority for government action.<sup>106</sup> Where the government has a property interest in the subject of the patent application (i.e., it relates to contract or research activities funded by a government agency), the Commissioner solicits the opinion of the funding agency and issues a secrecy order if notified that publication or disclosure of the information might be detrimental to the national security.<sup>107</sup> Where the government does not have a property interest, the advice of appropriate defense agencies is solicited when, in the Commissioner's opinion, disclosure might be detrimental to the national security.<sup>108</sup> If the defense agency determines that a secrecy order is justified, the Commissioner orders the material to be kept secret and a patent withheld.<sup>109</sup>

A patent secrecy order is issued for one year but is renewable annually if it is determined that the national interest requires continued nondisclosure.<sup>110</sup> The applicant has the right to seek compensation from the government for damages related to the imposition of the secrecy order and for the government's use, if any, of the information in question.<sup>111</sup>

The number of secrecy orders issued each year is relatively small. In fiscal year 1979, for example, 107,409 patent applications were received. Of these, 4,829 were forwarded to the defense agencies for review. Following that review, 243 secrecy orders were issued. Only forty-three of these involved patent applications that had not been classified for national security purposes, thereby indicating a prior governmental interest, when filed.<sup>112</sup> This authority has been reviewed by several courts but has not been challenged on first amendment grounds.<sup>113</sup>

#### E. *Trading With The Enemy and International Emergency Economic Powers Acts*

Under the Trading With The Enemy Act<sup>114</sup> and the International Emergency Economic Powers Act,<sup>115</sup> commercial exports to certain destinations of information of any nature may be controlled in times of war or national emergency. The Treasury Department administers these controls, some of which remain in effect.

---

106. *Id.* § 181.

107. *Id.*

108. *Id.*

109. *Id.*

110. *Id.*

111. *Id.* § 183.

112. See *The Government's Classification of Private Ideas: Hearings Before a Subcomm. of the House Comm. on Government Operations*, 96th Cong., 2d Sess. 2 (1980) (statement of Rene D. Tegtmeyer, Assistant Commissioner for Patents, Department of Commerce).

113. See, e.g., *Halpern v. United States*, 258 F.2d 36 (2d Cir. 1958).

114. 50 U.S.C. app. §§ 1-44 (1982 & Supp. I 1983).

115. *Id.* §§ 1701-1706.

### 1. Trading With The Enemy Act

The Trading With The Enemy Act (TEA)<sup>116</sup> gives the President broad powers to control trade with foreign countries. Prior to 1977, the statute granted these powers "[d]uring time of war or during any other period of national emergency declared by the President."<sup>117</sup> This provision was amended in 1977 to grant these powers only during the "time of war."<sup>118</sup> However, controls in place prior to that date may be extended annually by the President.<sup>119</sup> The relevant regulations have been extended repeatedly and were last extended by President Reagan until September 14, 1984.<sup>120</sup>

The TEA grants the President the authority to regulate any transactions in foreign exchange or credit, payments between banking institutions, and most other transactions involving gold or silver coin, bullion, currency, or securities.<sup>121</sup> He may also regulate or prohibit any transaction involving any property in which a designated foreign country or any of its nationals has any interest.<sup>122</sup> These powers apply to transactions involving any person or any property subject to the jurisdiction of the United States.<sup>123</sup> The TEA also grants the President broad powers over the property and interests of designated foreign countries or their nationals.<sup>124</sup> The combined effect of these authorities is to regulate all forms of commerce between the United States or its nationals and the designated "enemy" countries.

Regulations promulgated under this statute establish a foreign assets control system and prohibit, unless specifically authorized by the Secretary of the Treasury, a variety of transactions involving specific foreign countries.<sup>125</sup> The countries identified under this regulation at this time are North Korea, Cambodia, and North and South Vietnam.<sup>126</sup>

A variety of transactions are prohibited if they are effected by or on behalf of a designated country or its nationals, or if they involve property in which such a country or its nationals has any direct or indirect interest.<sup>127</sup> In addition, unless authorized by the Secretary of the Treasury, persons subject to U.S. jurisdiction

---

116. See *supra*note 114.

117. 50 U.S.C. app. § 5(b)(1) (1968).

118. Pub. L. No. 95-223, § 101(a), 91 Stat. 1625 (1977) (codified as amended at 50 U.S.C. § 5(b)(1). (1982 & Supp. I 1983).

119. Pub. L. No. 95-233, § 101(b), 91 Stat. 1625 (1977) (codified as amended at 50 U.S.C. app. § 5(b)(1) (1982 & Supp. I 1983).

120. Extension of the Exercise of Certain Authorities Under the Trading With the Enemy Act, 48 Fed. Reg. 40,695 (1983).

121. 50 U.S.C. app. § 5(b)(1) (1982 & Supp. I 1983).

122. *Id.*

123. *Id.*

124. *Id.*

125. 31 C.F.R. §§ 500.101-520.809 (1983).

126. *Id.* § 500.201(d).

127. *Id.*



may not purchase or otherwise engage in any transaction outside the United States involving materials originating in North Korea, Cambodia, or North and South Vietnam.<sup>128</sup> The definitions accompanying these prohibitions are drawn broadly.<sup>129</sup>

The Secretary of the Treasury may authorize the transactions described above by issuing a general or specific license.<sup>130</sup> General licenses, as with the EAA, take the form of regulatory exemptions.<sup>131</sup> Other transactions not authorized by general license require a specific license from the Office of Foreign Assets Control in the Treasury Department.<sup>132</sup>

In addition, the TEA regulations prohibit shipments to designated foreign countries of (a) materials on the Commerce Department's Commodity Control List; (b) materials whose unauthorized exportation from the United States is prohibited by regulations issued under the Mutual Security Act of 1954 (the Arms Export Control Act); and (c) materials or facilities relating to atomic energy whose exportation from the United States is prohibited under the Atomic Energy Act of 1954.<sup>133</sup> Unless authorized by the Secretary of the Treasury or his designee, no person within the United States may purchase or sell or arrange the purchase or sale of such materials in any foreign country or obtain any credit or payment from any banking institution in connection with any shipment of such materials from any foreign country directly or indirectly to Albania, Bulgaria, Cambodia, Czechoslovakia, Estonia, East Germany, East Berlin, Hungary, Latvia, Lithuania, North Korea, Outer Mongolia, People's Republic of China, Poland and Danzig, Romania, South and North Vietnam, Tibet, and the Soviet Union.<sup>134</sup> This approval requirement is in addition to the licensing and approval mechanisms established under the EAA, AECA, and AEA.

The regulations also control Cuban assets and all financial and commercial transactions involving Cuba, its nationals, or persons acting on their behalf.<sup>135</sup> The prohibitions regarding transactions involving Cuba or its nationals are virtually identical to those discussed above and prohibit any person subject to U.S. jurisdiction from dealing in materials originating in Cuba unless licensed by the Secretary of the Treasury.<sup>136</sup> These regulations also define "license," "general license," and "specific license" in the same manner as described above.<sup>137</sup>

Although the primary focus of the TEA and its implementing regulations is

128. *Id.* § 500.204.

129. *See id.* § 500.301.

130. *Id.* § 500.201.

131. *Id.* §§ 500.505-.535, 500.563-.565.

132. *Id.* §§ 500.318, 500.549-.562, 500.801.

133. *Id.* § 505.10.

134. *Id.* § 505.10.

135. *Id.* § 515.101-.809.

136. *Id.* § 515.204.

137. *Id.* § 515.316-.318.

on currency and material transactions, the operative provisions are sufficiently broad so as to control a wide range of transactions involving both "development" and "research" information. Unlike the control mechanisms discussed earlier, the TEA and its regulations pay little attention to public availability or intrinsic value.

## 2. International Emergency Economic Powers Act

The International Emergency Economic Powers Act (IEEPA)<sup>138</sup> was enacted in 1977 and provides the President with broad authorities, similar to those in the TEA, to regulate a wide variety of commercial and banking transactions involving persons or property subject to U.S. jurisdiction.<sup>139</sup> These authorities may be used when a "national emergency," as opposed to the state of war required under the TEA, has been declared to deal with an "unusual and extraordinary threat" to U.S. national security, foreign policy, or economic interests emanating in whole or substantial part from abroad.<sup>140</sup>

Congress must be notified when these authorities are exercised, and the emergency declaration terminates at the end of one year, unless renewed by the President.<sup>141</sup> This statutory authority has been invoked to impose restrictions on trade and currency transactions with Iran during the hostage crisis and was upheld by the courts in that context.<sup>142</sup> More recently, President Reagan used this authority to sustain the Export Administration Regulations when the EAA expired in October, 1983 and February, 1984.<sup>143</sup>

The IEEPA excludes from its terms, among other things, personal communications that do not involve a transfer of anything of value.<sup>144</sup> Thus, as in the TEA, "development" and "research" information in a commercial context by implication may fall within the regulatory structure created by the IEEPA.

---

138. 50 U.S.C. §§ 1701-1706 (1982 & Supp. I 1983).

139. *Id.* § 1702.

140. *Id.* § 1701.

141. *Id.* § 1703. The statute contains authority for Congress to act to end such a national emergency by adopting a concurrent resolution to that effect. Under *Immigration and Naturalization Service v. Chadha*, 103 S. Ct. 2764 (1983), however, this provision represents a form of invalid legislative veto.

142. *See Dames & Moore v. Regan*, 453 U.S. 654, 668 (1981) (an executive order involving emergency authority is "supported by the strongest presumptions and the widest latitude of judicial interpretation, and the burden of persuasion would rest heavily upon any who might attack it"); *United States v. Spawr Optical Research*, 685 F.2d 1076, 1080-81 (9th Cir. 1982), *cert. denied*, 103 S. Ct. 1875 (1983) (upholding presidential authority to continue controls under an executive order and the Trading With The Enemy Act, IEEPA's predecessor, during a lapse in the EEA); H. R. REP. No. 459, 95th Cong., 1st Sess. 13 ("Should a lapse [of the EEA] occur, however, the authority of Title II of [IEEPA] could be used to continue the Export Administration Regulations in effect if, and to the extent that, the President declared a national emergency. . . .") (referring to H.R. 7738).

143. *See supra* note 21.

144. 50 U.S.C. § 1702(b) (1982 & Supp. I 1983).

#### IV. CONCLUSION

There exists a large, complex, and ambiguous body of statutes and regulations that govern, or have the potential for governing, the export of various types of technical information in many circumstances. These controls are based on the nature of the information to be exported, its destination, and its practical application. Attorneys advising clients in trade matters should be aware of these authorities and alert for issues in these areas. To be content to focus on exports of hardware, products, or equipment is to risk damaging consequences for both the country and the client.