Essay

Between a Rock and a Hard Place: The Export of Technical Data Under the International Traffic in Arms Regulations

Mollie McGowan*

Introduction

The export of defense-related technical data[1] has garnered significant attention in recent years.[2] Factors such as outsourcing, the increasing ease of transferring technical data, the globalization of manufacturing, and the upsurge in the number of foreign nationals employed by U.S. companies in technology and defense-related fields have all contributed to the rapid rise in the export of defense-related technical data by U.S. companies.[3] This rise, in turn, has led to stringent technical-data export regulations[4] that have made technical data

* J.D., 2008, The George Washington University Law School. I would like to thank Professor Michael Abramowicz for his assistance and suggestions. I would also like to thank my family for their support and encouragement.

1 "Technical data" includes information required for the "design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles" including "blueprints, drawings, photographs, plans, instructions or documentation" as well as classified information and software relating to defense articles and services. 22 C.F.R. § 120.10 (2007).

2 *See* Christopher R. Wall, *Controlling the Flow of Technology in Global Operations: Deemed Exports*, *in* Coping with U.S. Export Controls 2006, at 211, 213 (PLI Commercial Law & Practice, Course Handbook Series No. 8696, 2006).

3 *See* Wall, *supra* note 2, at 213; *see also* Giovanna M. Cinelli, Outsourcing—Is It Really Worth the Cost? 1 (2005), http://www.pattonboggs.com/news/detail.aspx?news=201 (follow "OUTSOURCING—IS IT REALLY WORTH THE COST?" hyperlink).

4 *See* International Traffic in Arms Regulations (ITAR), 22 C.F.R. §§ 120–130 (2007).

exchanges between and within companies very cumbersome.[5] To further complicate the situation, recent developments have forced U.S. companies to account not only for the *actual* export of technical data but also for the *potential* export of technical data.[6]

In exploring how these changes have tightened the regulatory grip on the export of technical data, this Essay discusses the difficulty faced by U.S. companies in limiting their exposure to potential criminal or civil penalties. Part I surveys the background and definitions associated with the export of technological data. Part II examines recent developments in technological exports—namely, charges brought by the U.S. State Department against General Motors—that have changed the export landscape. Part III addresses the aftermath of the General Motors case, while Part IV offers advice on how companies can avoid similar enforcement actions by the State Department.

I. Background

A. Definitions

"Exporting" technological data may seem like a strange concept. Just as physical items, such as packages, can be shipped from the United States to another country, so too can technical data be "shipped" abroad. For example, a technical data file can be transmitted to a foreign country via e-mail, and it may require an export license just like the physical package.[7] Technical data, however, may also be considered "exported" to another country when it is simply "released" or "transferred" to a foreign national.[8] Such an export can take place when the foreign national is abroad or in the United States, and it may also require an export license.[9]

The State Department's Directorate of Defense Trade Controls ("DDTC") implements the International Traffic in Arms Regulations ("ITAR") to regulate exports of defense-related merchandise, services, technology, and technical data designated on the U.S. Munitions List ("ML").[10] Generally, technology and related items are "included in the ML when they are designed principally for military, as opposed

---

5 *See* Wall, *supra* note 2, at 213.

6 Linda M. Weinberg & Lynn Van Buren, *The Impact of U.S. Export Controls and Sanctions on Employment*, 35 PUB. CONT. L.J. 537, 545 (2006).

7 Wall, *supra* note 2, at 213.

8 22 C.F.R. § 120.17(a)(4); *see also* Wall, *supra* note 2, at 213.

9 22 C.F.R. § 120.17(a)(4); *see* Wall, *supra* note 2, at 213.

10 22 C.F.R. § 120.1; *see also* Christopher F. Corr, *The Wall Still Stands! Complying with Export Controls on Technology Transfers in the Post-Cold War, Post-9/11 Era*, 25 HOUS. J. INT'L L. 441, 464 (2003); Wall, *supra* note 2, at 215.

to commercial, applications."[11] Under the ITAR, a license is required for the export of defense-related technical data.[12]

The ITAR provides definitions for three important export control terms: export, foreign person, and technical data. Under ITAR § 120.17, export includes "disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad."[13] ITAR § 120.16 defines "foreign person" as "any natural person who is not a lawful permanent resident as defined by 8 U.S.C. § 1101(a)(20) or who is not a protected individual as defined by 8 U.S.C. § 1324b(a)(3)."[14] "Technical data" under ITAR § 120.10 is defined broadly to include information "required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles" including "blueprints, drawings, photographs, plans, instructions or documentation."[15] The definition also encompasses classified information and software relating to defense articles and services.[16]

B. Export of Technical Data Under the ITAR

Under the ITAR, an export of technical data can occur in various situations. An export may occur when a corporation makes an intracompany transfer of ITAR-controlled technical information to its subsidiary in another country.[17] Exporting technical data can also take place when a company transfers[18] controlled technical data to one of its own employees in the U.S. or abroad if that employee is a foreign national.[19] A third way a company can export technical data is by transferring information to companies or individuals to whom it has outsourced certain services, such as information technology or

---

11 Corr, *supra* note 10, at 464.

12 *See* 22 C.F.R. §§ 125.2, 125.3.

13 22 C.F.R. § 120.17.

14 22 C.F.R. § 120.16. Under 8 U.S.C. § 1101(a)(20), the term "lawfully admitted for permanent residence" is defined as "the status of having been lawfully accorded the privilege of residing permanently in the United States as an immigrant in accordance with the immigration laws, such status not having changed." 8 U.S.C. § 1101(a)(20) (2000). The ITAR's definition of "foreign person" also encompasses "any foreign corporation, business association, partnership, trust, society or any other entity or group that is not incorporated or organized to do business in the United States, as well as international organizations, foreign governments and any agency or subdivision of foreign governments (e.g., diplomatic missions)." 22 C.F.R. § 120.16.

15 22 C.F.R. § 120.10.

16 *Id*.

17 Wall, *supra* note 2, at 214.

18 In addition to transfer, exporting also includes oral or visual disclosure. 22 C.F.R. § 120.17.

19 Wall, *supra* note 2, at 214.

software development, if those companies or individuals are considered to be foreign nationals.[20] Finally, technical data can be "exported" to a foreign national through visual inspection or oral discussion.[21] Under ITAR § 125.2(c), "a license is [even] required for the oral, visual or documentary disclosure of technical data by U.S. persons to foreign persons. . . . A license is required for such disclosures in connection with visits to foreign diplomatic missions and consular offices."[22]

The complicated web of situations in which U.S. companies risk export of ITAR-controlled technical data places a heavy burden on companies that have foreign subsidiaries, employ foreign nationals, or outsource to foreign companies or foreign persons. This heavy burden stems primarily from three factors: (1) the ITAR's cumbersome licensing requirements, (2) its often inefficient license processing, and (3) the risk of significant penalties if a company fails to comply with ITAR licensing.[23]

Regarding its licensing requirements, the ITAR requires that any person or company intending to export ITAR-controlled technical data "must obtain the approval of the Directorate of Defense Trade Controls prior to the export."[24] Therefore, in order to comply with the ITAR, a company must classify all of its technology in order to determine whether it would require a license if released to a foreign national.[25] A company is also obligated to determine the nationality or immigration status of all employees to whom it plans to transfer or export ITAR-controlled data.[26] Based on these assessments, a company must then restrict the type of technical data that may be transferred to foreign national employees, or obtain licenses from the DDTC for those employees. Further, if an employee is a national of a proscribed country under ITAR § 126.1, such as Cuba, Iran, or North Korea, the employer can neither obtain an export license for that employee nor export ITAR-controlled technical data to that employee.[27]

---

20 *Id*.

21 22 C.F.R. § 125.2(c).

22 *Id.*

23 *See* Wall, *supra* note 2, at 214. Under 22 U.S.C. § 2778(c), "[a]ny person who willfully violates any provision of this section . . . or any rule or regulation issued under [this] section . . . shall upon conviction be fined for each violation not more than $1,000,000 or imprisoned not more than ten years, or both." 22 U.S.C. § 2778(c) (2000).

24 22 C.F.R. § 123.1(a).

25 Wall, *supra* note 2, at 214.

26 *Id.* at 215.

27 The ITAR does not provide an exception for foreign nationals from these countries who possess security clearance or similar authorization. U.S. policy under ITAR § 126.1(a) is to

Therefore, companies may have to go as far as restricting the type of technical data their employees can disclose to one another even when they are working side by side in the office or laboratory.[28]

To add to the burden of extensive licensing requirements, the DDTC has a longstanding reputation as being nontransparent, inaccessible, and plagued by licensing delays.[29] Companies must simply deal with this burden, however, because failure to obtain a license for ITAR-controlled technical information could result in criminal penalties, including a fine of $1,000,000 and/or ten years in prison; civil penalties; or debarment.[30] Therefore, taking steps to limit foreign national employees' access to ITAR-controlled information, or obtaining the proper licenses for those employees' access, is crucial to avoiding discipline by the State Department.

II. Recent Developments

The implications of a recent enforcement action by the State Department against General Motors Corporation ("GM") and General Dynamics Corporation ("GD") have further complicated the issue of exporting ITAR-controlled technical data.[31] In the GM and GD enforcement action, the State Department charged GM with violating 22 C.F.R. § 127.1(b) for providing

> unauthorized *access* to U.S. technical data to foreign national employees including foreign persons from proscribed countries by failing to account for the acts of its employees, agents, and all authorized persons to whom possession of the licensed defense articles or technical data has been entrusted regarding the operation, use, possession, transportation, and handling of such defense article or technical data.[32]

"deny licenses and other approvals for exports and imports of defense articles and defense services, destined for or originating in certain countries. . . . [E]xemptions provided in the regulations in this subchapter . . . do not apply with respect to articles . . . for export to any proscribed countries . . . ." 22 C.F.R. § 126.1(a).

28 *See* Wall, *supra* note 2, at 214.

29 *See* Corr, *supra* note 10, at 464–65.

30 22 U.S.C. § 2278(c) (2000); 22 C.F.R. §§ 127.1, .3, .7, .10.

31 *See* Draft Charging Letter from David C. Trimble, Dir., Def. Trade Controls Compliance, to Artis M. Noel, Counsel, Gen. Motors Corp. & David A. Savner, Senior Vice President & Gen. Counsel, Gen. Dynamics Corp., *available at* http://www.pmddtc.state.gov/Consent_Agreements/2004/General_Motors_CorpandGeneral_Dynamics_Corp/Draft_Charging_Letter.pdf [hereinafter Draft Charging Letter].

32 Draft Charging Letter, *supra* note 31, at 15 (emphasis added). ITAR § 126.1(a) states that no export licenses shall be granted to export ITAR-controlled information to certain countries, such as Cuba, Iran, and North Korea, or to countries, such as China, under an arms embargo by the United States. 22 C.F.R. §126.1(a).

According to the State Department's Draft Charging Letter, GM provided unauthorized access to ITAR-controlled technical data because many of GM's engineering and other technical support personnel, including foreign persons, dual nationals, and foreign persons from proscribed countries, had computers with access to programs and/or drives that contained most of the GM defense technical data.[33] To put it simply, GM was charged with providing foreign persons with unauthorized "access" to ITAR-controlled data.[34]

Although the State Department's enforcement action charged GM with a violation, it failed to resolve one critical ambiguity. It remains unclear whether a potential violation of the ITAR alone, based solely on a company providing access to technical data without *actual* disclosure or transfer to a foreign person, is sufficient to support a penalty under the ITAR. ITAR does not specifically address whether simply providing a foreign national with access to ITAR-controlled technical data violates the ITAR.[35] The State Department has never instituted an enforcement action against a company based solely on that company's providing foreign nationals with access to ITAR-controlled technical data,[36] and it is questionable whether the State Department is authorized to prosecute potential violations of the ITAR solely on this basis.

III. The Aftermath of GM: The State Department's Authority to Prosecute Potential ITAR Violations

Three main questions stem from the GM enforcement action: (1) whether the State Department has the authority to prosecute potential violations of the ITAR, (2) whether it will prosecute such potential violations, and (3) what companies should do to protect themselves.

---

33 Draft Charging Letter, *supra* note 31, at 7.

34 *Id*.

35 *See* 22 C.F.R. §§ 120–130. There is a difference between transfer and access. To illustrate, transferring technical data is like handing someone a physical document containing the data. Providing access to that data is failing to maintain the data in a secure manner. For instance, giving someone a key to the company headquarters so they can clean up the office and organize the company files, but failing to seal or adequately protect sensitive documents that the person may come across in the process, would constitute providing access. *See* Weinberg & Van Buren, *supra* note 6, at 545.

36 *See, e.g.*, Weinberg & Van Buren, *supra* note 6, at 545 (stating that the recent concern regarding access to technical data "stems from" the GM and GD enforcement matter while citing no case law).

A. Authority of the State Department and the DDTC Under the Arms Export Control Act and the ITAR

Section 38 of the Arms Export Control Act ("AECA"), codified at 22 U.S.C. § 2778, gives the President the authority to "control the import and export of defense articles and defense services" and to "designate those items which shall be considered as defense articles and defense services . . . and to promulgate regulations for the import and export of such articles and services."[37] The AECA does not specifically define the meaning of "export."[38]

The statutory authority of the President to promulgate regulations relating to the export of defense articles and defense services was delegated to the Secretary of State under Executive Order 11,958.[39] ITAR § 120.1 implements that authority.[40] Under the delegation authority of the Secretary of State, these regulations are "primarily administered by the Deputy Assistant Secretary for Defense Trade Controls and Managing Director of Defense Trade Controls, Bureau of Political-Military Affairs."[41] Under ITAR § 120.17(a)(4), the definition of export includes "[d]isclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad."[42]

Under these provisions of the AECA and the ITAR, it is unclear whether the State Department has the authority to prosecute U.S. companies for simply providing foreign persons access to ITAR-controlled technical data. This issue has yet to come before the courts.[43] If a court were to assess the authority of the State Department in this situation, however, it would find guidance in *Bowles v. Seminole Rock & Sand Co.*[44] and *Auer v. Robbins*.[45]

B. Seminole Rock *and* Auer *Deference*

A court would look to *Seminole Rock* and *Auer* in order to assess whether to defer to the DDTC's interpretation of export contained in

---

37 22 U.S.C. § 2778(a) (2000).

38 *Id*.

39 22 C.F.R. § 120.1. *See* Exec. Order No. 11,958, 42 Fed. Reg. 4311 (Jan. 18, 1977).

40 22 C.F.R. § 120.1.

41 22 C.F.R. § 120.1(a).

42 22 C.F.R. § 120.17(a)(4).

43 *See, e.g.*, Weinberg & Van Buren, *supra* note 6, at 545 (citing only the GM and GD enforcement matter, and not actual cases, in support of its observation that practitioners just recently started focusing on access to technical data by foreign national employees).

44 Bowles v. Seminole Rock & Sand Co., 325 U.S. 410 (1945).

45 Auer v. Robbins, 519 U.S. 452 (1997).

the Draft Charging Letter as an agency interpretation of its own regulation.[46] Congress did not expressly define export in the AECA, nor did it specify whether providing foreign nationals with access to defense-related technical data qualifies as an export under the AECA.[47] Again, under the ITAR, the DDTC defines export to include "[d]isclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad."[48] The DDTC's more expansive understanding of export found in its Draft Charging Letter, interpreting export to include providing foreign nationals with access to ITAR-controlled technical data,[49] seems to be a further interpretation of the definition of export contained in the ITAR, its own regulation.

Under *Seminole Rock*, an agency's construction of its own regulation "becomes of controlling weight unless it is plainly erroneous or inconsistent with the regulation."[50] Some courts have described *Seminole Rock* and *Auer* deference as even greater than the level of deference given to an agency's interpretation of ambiguous terms in a statute.[51] Therefore, if *Seminole Rock* and *Auer* deference apply in this case, a great amount of deference would be given to the DDTC's interpretation of export within its own statute.[52] Only if a court decided that the DDTC's construction of the ITAR was "plainly erroneous or inconsistent with the regulation" would the court refuse to defer to the DDTC.[53]

In order for *Seminole Rock* and *Auer* deference to apply, however, certain criteria must be met. *Seminole Rock* and *Auer* deference will only apply here if (1) the ITAR itself is ambiguous;[54] and (2) the DDTC's interpretation of export in the Draft Charging Letter, as including providing foreign persons with access to ITAR-controlled in-

---

46 *See Seminole Rock*, 325 U.S. at 414; *Auer*, 519 U.S. at 461.

47 *See* 22 U.S.C. § 2778 (2000).

48 22 C.F.R. § 120.17(a)(4) (2007).

49 *See* Draft Charging Letter, *supra* note 31, at 4, 15.

50 *Seminole Rock*, 325 U.S. at 414.

51 *See, e.g.*, C.F. Commc'ns Corp. v. FCC, 128 F.3d 735, 738 (D.C. Cir. 1997); *see also* GARY LAWSON, FEDERAL ADMINISTRATIVE LAW 452 (4th ed. 2007).

52 *See Seminole Rock*, 325 U.S. at 414.

53 *See id*.

54 Christensen v. Harris County, 529 U.S. 576, 588 (2000) ("*Auer* deference is warranted only when the language of the regulation is ambiguous."); *see also* Chevron U.S.A. Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837, 843 (1984) (stating that ambiguity in a statute is necessary before a court will give deference to an agency interpretation).

formation, is sufficiently concrete and formal to be recognized as the DDTC's official position on the meaning of export.[55]

Under the first criterion, the DDTC's definition of export contained in the ITAR includes "[d]isclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad."[56] The regulations do not, however, further define "disclosing" or "transferring"—terms that could be seen as ambiguous. Therefore, this leaves room for the DDTC to interpret its own regulation.

Under the second criterion, neither *Seminole Rock* nor *Auer* provides a specific test as to when an agency's interpretation of its own regulation is formal enough to trigger *Seminole Rock* or *Auer* deference. However, in light of the Supreme Court's holding in *Christensen v. Harris County*[57] that a certain level of formality in an agency interpretation is required to trigger *Chevron* deference,[58] it seems that a certain level of formality would also be necessary for *Seminole Rock* and *Auer* deference.[59]

Furthermore, *Seminole Rock* and *Auer* do provide some guidance as to the level of formality required before a court will give deference to an agency's interpretation of its regulation.[60] In *Seminole Rock*, the main issue in the case involved the Office of Price Administration's interpretation of the meaning of the phrase "highest price charged during March, 1942" in a regulation it had issued.[61] The Office of Price Administration had issued a bulletin at the same time it promul-

---

55 *See Christensen*, 529 U.S. at 587 (stating that a certain level of formality is necessary for an agency's interpretation to receive *Chevron* deference and implying that an agency interpretation, in general, requires a certain level of formality in order to receive judicial deference).

56 22 C.F.R. § 120.17(a)(4) (2007).

57 Christensen v. Harris County, 529 U.S. 576, 588 (2000).

58 *See Christensen*, 529 U.S. at 587.

59 Because *Auer* deference is warranted only when the language of a regulation is ambiguous, just as *Chevron* deference is warranted only when the language of a statute is ambiguous, it would follow that because a certain level of formality (either a formal adjudication or notice and comment rulemaking) is required for an interpretation to receive *Chevron* deference, a certain level of formality would also be required for an interpretation to receive *Auer* deference. Otherwise, an agency easily could get around the formalities required for *Chevron* deference, and receive *Auer* deference, by simply continuously reinterpreting its own regulations at any point in time. Not only would this provide a loophole for agencies, but it would also deprive the public of any type of notice as to the agency's formal position on numerous topics.

60 *See* Auer v. Robbins, 519 U.S. 452, 458–59 (1997); Bowles v. Seminole Rock & Sand Co., 325 U.S. 410, 415–17 (1945).

61 *See Seminole Rock*, 325 U.S. at 415.

gated the regulation at issue in that case, which was made available to regulated manufacturers, wholesalers, and retailers.[62]

In the bulletin, entitled *What Every Retailer Should Know About the General Maximum Price Regulation*, the Administrator of the Office of Price Administration clearly stated that "[t]he highest price charged during March 1942 means the highest price which the retailer charged for an article *actually delivered* during that month or, if he did not make any delivery of that article during March, then his *highest offering price* for delivery of that article during March."[63] The Administrator also gave the same interpretation of "highest price charged during March, 1942" in a quarterly report to Congress.[64] The Court in *Seminole Rock* stated that "[a]ny doubts concerning this interpretation of [the relevant phrase] are removed by reference to the administrative construction" and deferred to the agency's interpretation of its regulation.[65]

In *Auer*, the Court examined whether the Secretary of Labor's interpretation of the "salary basis test," laid out in regulations promulgated by the Secretary, was a valid interpretation of the regulations.[66] The Secretary of Labor's interpretation was outlined in an amicus brief to the *Auer* Court.[67] Petitioners in the case argued that an interpretation in the form of an amicus brief should not be entitled to deference.[68] The *Auer* Court accepted the interpretation, however, stating that "[t]he Secretary's position is in no sense a post hoc rationalizatio[n] advanced by an agency seeking to defend past agency action against attack."[69] The Court went on to say that there was no reason to suspect that the Secretary's interpretation failed to "reflect the agency's fair and considered judgment on the matter in question."[70]

The acceptance of relevant agency interpretations in *Seminole Rock* and *Auer* as concrete enough to apply deference creates tentative guidelines as to the level of formality of an agency's interpretation required to trigger *Seminole Rock* and *Auer* deference. In *Seminole Rock*, an agency interpretation clearly defined in a bulletin issued

---

62 *See id.* at 417.

63 *Id.* (quotation omitted).

64 *Id.*

65 *Id.*

66 *See* Auer v. Robbins, 519 U.S. 452, 455 (1997).

67 *Id.* at 461.

68 *See id.* at 462.

69 *Id.* (quotation omitted).

70 *Id.*

along with the regulation at issue, in combination with a similar interpretation in a quarterly report to Congress, was clear and concrete enough to receive deference.[71] In *Auer*, the Court accepted an amicus brief as a clear and concrete agency interpretation of its statute.[72] The *Auer* Court also implied that in order for an agency interpretation to get *Seminole Rock* and *Auer* deference, (1) the interpretation could not be a "post hoc rationalization" crafted to defend an agency in litigation, and (2) the interpretation must be deemed to "reflect the agency's fair and considered judgment on the matter in question."[73]

Based on *Seminole Rock* and *Auer*, if an agency issues a written statement in order to establish its interpretation of its own regulation that reflects the agency's "fair and considered judgment" on the matter at hand, and such a statement is not a "post hoc rationalization" crafted to defend the agency in litigation, the agency will receive *Seminole Rock* and *Auer* deference for its interpretation. In this case, no such statement of the DDTC's interpretation of export under the ITAR exists, as the only evidence of the DDTC's position as to export comes from the Draft Charging Letter the DDTC issued to GM.[74]

The DDTC's interpretation of export in the Draft Charging Letter as including providing foreign persons with access to ITAR-controlled information is not clear and concrete enough to warrant *Seminole Rock* and *Auer* deference. The interpretation is simply inferred from the charges in the Draft Charging Letter[75] rather than gleaned from a written statement issued by the agency for the purpose of establishing its official position, as was the case in *Auer* and *Seminole Rock*.[76] Although the DDTC's interpretation of export in the Draft Charging Letter is not a "post hoc rationalization" crafted for litigation, it is unclear that this interpretation is the agency's actual position, and it does not seem to "reflect the agency's fair and considered judgment on the matter in question."[77] The agency's position is unclear, even though the DDTC charged GM with providing "unauthorized access to U.S. technical data to foreign national employ-

---

71 *See* Bowles v. Seminole Rock & Sand Co., 325 U.S. 410, 417 (1945).

72 *See Auer*, 519 U.S. at 462.

73 *Id*.

74 *See* Draft Charging Letter, *supra* note 31, at 15; *see also* Weinberg & Van Buren, *supra* note 6, at 545 (stating that the recent concern regarding access to technical data "stems from" the GM and GD).

75 *See* Draft Charging Letter, *supra* note 31, at 4, 15.

76 *See Auer*, 519 U.S. at 462; *Seminole Rock*, 325 U.S. at 417.

77 *Auer*, 519 U.S. at 462.

ees,"[78] because it charged GM with six other violations of the ITAR, including the "actual transfer" of technical data to foreign nationals, an action clearly defined as an export in the ITAR.[79] Further, the agency did not specify what charges led to its imposition of a $20 million fine on GM.[80] Overall, because the DDTC's position was only set forth in a draft charging letter rather than in a written statement intended to establish its official position on the matter, it is not clear that the interpretation is a result of "fair and considered judgment" on the part of the DDTC. Nor is it clear that the DDTC intends this to be its formal position on the meaning of export.

It is also unclear whether the DDTC's interpretation of export in the Draft Charging Letter is its actual position. The interpretation was not explicitly stated in the letter but instead had to be inferred from the way the DDTC handled 248 charges against GM and GD.[81] Therefore, it may be too early to examine the propriety of such an interpretation. In order to complete the analysis, however, this Essay will assume that the DDTC's formal position is that export under the ITAR includes providing foreign persons with access to ITAR-controlled technical data, allowing the DDTC to prosecute companies for such "exports."

Assuming that this is the DDTC's position, and assuming it has not been stated at a level of formality required to warrant deference from a court under *Seminole Rock* and *Auer*, the next step is to examine the DDTC's definition of export *de novo*.[82] Looking exclusively at the language of the AECA, there is no specific definition of "export."[83] Under the statute, the term export seems to encompass the natural, commonly understood dictionary definition of export: "[t]o send or transport (a commodity, for example) abroad, especially for trade or sale."[84] The plain meaning of the statute,[85] along with legislative history,[86] provide no positive support for an argument that it was the intent of Congress to stretch the definition of export to in-

78 Draft Charging Letter, *supra* note 31, at 15.

79 *Id.* at 14; *see* 22 C.F.R. § 120.17(a)(4) (2007).

80 *See* General Motors Corporation & General Dynamics Corporation 2 (Bureau of Political–Military Affairs, U.S. Dep't of State, Nov. 1, 2004) (final order), *available at* http://www.pmddtc.state.gov/Consent_Agreements/2004/General_Motors_CorpandGeneral_Dynamics_Corp/Order.pdf.

81 *See* Draft Charging Letter, *supra* note 31, at 4, 15.

82 *See* Chevron U.S.A. Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837, 843 (1984).

83 *See* 22 U.S.C. § 2778 (2000).

84 THE AMERICAN HERITAGE DICTIONARY 626 (4th ed. 2000).

85 *See* 22 U.S.C. § 2778.

86 *See* H.R. REP. NO. 94-1272 (1976).

clude providing foreign nationals with access to defense-related technical data. Additionally, under the ITAR (the DDTC's formal interpretation of export that would receive *Chevron* deference), the DDTC already stretches the meaning of export to include "[d]isclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad."[87]

It could be argued that within the ITAR's definition of "export," "disclose" includes providing access. However, to provide access is not a common understanding of disclose, nor is it part of the dictionary definition, which is "to expose to view, as by removing a cover; uncover."[88] Therefore, based on the fact that the DDTC's definition of export clearly stretches the meaning of export intended by Congress,[89] and the fact that the definition of export in the Draft Charging Letter stretches the ITAR definition even further,[90] *de novo* review of the definition gleaned from the Draft Charging Letter would likely lead a court to conclude that this is not a proper interpretation of "export." Based on this analysis, it would be improper, and outside of the DDTC's authority, to punish companies for providing such access to foreign nationals.

IV. Safeguards Companies Should Take to Protect Themselves from Prosecution of Potential ITAR Violations for Providing Foreign Nationals with Access to ITAR-Controlled Technical Data

It remains unclear whether it is actually the DDTC's formal position that "export" under the ITAR includes providing foreign nationals with access to defense-related technical data. Still, though, companies should take steps to protect themselves from the possibility that such an interpretation of export is enforceable under the ITAR, even though a court would likely hold that interpretation to be unreasonable if it were the DDTC's formal position. In order to protect themselves, companies could theoretically obtain export licenses from the DDTC for all of the foreign nationals (not from proscribed countries)[91] to whom they intend to provide access to ITAR-controlled

---

87 22 C.F.R. § 120.17(a)(4) (2007).

88 THE AMERICAN HERITAGE DICTIONARY, *supra* note 84, at 515. Note that to uncover is different from failing to take sufficient precautions, such as covering in the first place.

89 Congress did not even define export, implying that the common meaning of the word was its understood meaning. *See* 22 U.S.C. § 2778(g).

90 *See* Draft Charging Letter, *supra* note 31, at 4, 15.

91 No export license can be obtained for export to countries or foreign persons from countries prohibited from obtaining U.S. exports. 22 C.F.R. § 126.1.

technical data, through the companies' computer system or otherwise.[92] This option, however, may not be feasible because, according to a legal practitioner in international trade,[93] the DDTC has refused to license potential exports and will not provide export licenses for foreign nationals who merely have access to ITAR-controlled technical data.[94]

In light of this, the best option for companies employing or outsourcing to foreign persons is to restrict the access of those persons to ITAR-controlled technical data.[95] Unfortunately, this puts companies between a rock and a hard place. When ITAR-controlled technical data is stored on a single, company-wide computer system, restricting access can be almost impossible.[96] To attempt to sufficiently restrict access, the company should classify all technical data to determine what is ITAR-controlled and then develop some sort of system-wide, password-controlled, access-control mechanism that would restrict foreign nationals from accessing relevant technical data.[97] Creating such an elaborate system, however, is not an easy task, and it will be extremely expensive and infeasible for many companies.[98]

Other options may include extensive employee education about the ITAR and the access issues it presents or simply refraining from hiring or outsourcing to foreign persons. Unfortunately, none of these options presents an easy answer to the problem. Until the DDTC gives an official position on the meaning of the term export, companies should take steps to protect themselves, rather than face criminal or civil penalties such as extensive fines[99] and possible debarment from future exports under the ITAR.[100]

Conclusion

In today's world of increasing technology use, globalization, and outsourcing, many companies are greatly affected by the DDTC's license requirements for exporting technical data. The recent develop-

---

92 *See* 22 C.F.R. § 123.1.

93 The source of this information asked to remain anonymous. No actual documentation exists for this assertion.

94 The DDTC's position on refusing to issue licenses for providing access to ITAR-controlled technical data also implies that it is not the DDTC's official position that export includes merely providing access to ITAR-controlled technical data.

95 *See* Corr, *supra* note 10, at 523–24; Wall, *supra* note 2, at 222–23.

96 Wall, *supra* note 2, at 222.

97 *Id*. at 223.

98 *Id*.

99 *See* 22 U.S.C. § 2778(c) (2000); 22 C.F.R. § 127.3 (2007).

100 *See* 22 C.F.R. § 127.7.

ments surrounding the GM case, and the possibility that the DDTC will prosecute companies for simply providing foreign nationals with access to ITAR-controlled technical data, impose the huge burden on many U.S. companies of guarding against unlicensed technology exports. Until the DDTC's interpretation of export is made clear, however, affected companies must simply take all necessary precautions to avoid prosecution by the DDTC.