Allies at Sixes and Sevens: Sticky Issues in Australian – US Defence Trade Controls

Roland L. Trope and Dr. Monique Witt[1]

The article explains the rationale of United States' International Traffic in Arms Regulations (ITAR). It argues that the current Australian effort to procure waivers or relaxations of ITAR requirements is misplaced. The best way to facilitate Australian access to advanced US military technology is for Australia to tighten its regulatory and contractual measures to reduce the perceived risk of unauthorized intangible transfers of sensitive data.

Australia is one of the United States' most dependable and capable allies. Hence, any significant regulatory obstacle to interoperability of Australian and US forces does not serve the interests of either party. But there is a spectrum of defence export control issues that currently impede the full military and strategic cooperation of Australia and the US. This article aims to help the US and Australia achieve their joint strategic goals by explaining the rationale for the US controls, illustrating how they work in practice, and suggesting steps Australia might take to facilitate access to US technology within this framework.

International Traffic in Arms Regulations

The defence export approval process is complex, detailed, and time-intensive. When approvals are granted they are often more limited in scope than Australia requested. Such incomplete grants become particularly significant when a decision to purchase US equipment is predicated on the belief that a particular weapon platform (and onboard system) enjoys a technological advantage. Such a technological edge can be wholly dependent on software/hardware or protocol compatibility, on specialized training in the use of such equipment, on delivery of the full range of equipment, or simply on access to a system's software codes. If the delivered equipment does not contain the full complement of capabilities, the anticipated technological advantage may prove illusory.

Moreover, if such equipment does not include US approvals for full access to technical data, this could prevent the Australian purchaser from modifying and/or updating software to optimize it for Australian operational use (or

[1] The views expressed in this article are solely those of the authors, and should not be attributed to the United States Military Academy, the US Department of Defense or the United States Government.

prevent it from doing so without violating the conditions of its licensed export). It could also limit the purchaser's ability to maintain and repair the equipment. Australia's decisions not to purchase the F-22, and instead to allocate its resources to the Joint Strike Fighter (JSF) illustrates the high stakes involved. As Australia's Minister of Defence, the Hon. Dr. Brendan Nelson observed:

> The reason we're not asking for the F-22 is because, whilst it is a brilliant air-to-air combat fighter, Australia needs 100 aircraft. We need a great all-rounder [the JSF]; it can bat and it can bowl, it can do air-to-air combat and strike capability. … It's the five percent of this aircraft's capability that is classified to which I have had privileged access, and that's the five percent that really counts. And that's why this is the correct aircraft for us…[2]

Consider the difficulties that would be created if restrictions on tech transfers related to the JSF limited or impeded the use of that crucial 5%. Australia might have serious misgivings. Even if these transfers were ultimately authorized, it is clear that time considerations are paramount in the purchase and deployment of military equipment, particularly for aircraft that must be phased in before aging aircraft are retired.[3] Such delays are detrimental not only to Australia (in obtaining aircraft suited to its needs), but also to the US (which counts on Australia's combat readiness). Clearly, while maximizing its access to essential US technical data Australia must recognize the very real security concerns of protecting highly sensitive military technology that underlie the applicable US defence trade control regulations—the International Traffic in Arms Regulations (ITAR). A better understanding of ITAR will improve the likelihood that Australia receives the tech transfers essential to its operational readiness.

Recent efforts by Australia (and Canada) have led to some concessions on ITAR prohibitions regarding access to technical data by foreign nationals. However, such concessions will not ensure that Australia receives the full complement of a requested tech transfer. The US government remains highly (and justifiably) concerned that unauthorized access to, and unauthorized releases of, sensitive technical data could seriously jeopardize its national security. And such concerns have intensified in response to recent security breaches by US defence contractors.[4]

---

[2] *Transcript of 60 Minutes Program, "Dogfight,"* 18 March 2007, <http://sixtyminutes.ninemsn.com.au/article.aspx?id=259495> [Accessed 6 June 2007].

[3] For example, the need to avert a gap in Australia's air combat capability, between retirement of its fleet of F-111's and the delivery of sufficient quantities of Joint Strike Fighter, reportedly motivated Australia's recent decision to purchase 24 F/A-18F Block II Super Hornets. See The Hon. Dr. Brendan Nelson, Minister for Defence, Media Release, *$6 Billion to Maintain Australian Regional Air Superiority*, March 6, 2007, <http://www.minister.defence.gov.au/NelsonMintpl.cfm?CurrentId=6437> [Accessed 6 June 2007].

[4] Examples from cases concluded in 2006 and 2007 include the Boeing Company's alleged unauthorized exports of QRS-11 quartz rate sensors to the People's Republic of China

In the post-9/11 environment, substantial contracts have been awarded for urgently needed equipment and for research and development to increase the US technological edge. However, this has put much sensitive, advanced military technology in the hand of civilian contractors, creating a more porous security environment.[5] While private sector profit motives encourage development of cutting-edge technology, this occurs at the expense of full control of the dissemination of, and access to, such technology. This is the risk that ITAR addresses.

US security concerns have increasingly focused on the ease with which breaches can occur through downloads to portable, digital media, and uploads and transfers through the Internet – so-called "intangible transfers." Increasingly, digital communication protocols, and the efficiencies that these create, make it easier to breach export controls or to render such controls ineffectual. Given the increasing need to protect US defence technology, and the increasing risk of inadvertent transfer to prohibited destinations, we believe that Australian defence contractors will improve their chances of receiving needed technology and related data by enhancing their own internal controls on dissemination of sensitive data. By either mirroring the level of security required by the US, or demonstrating an understanding of the policy concerns involved in ITAR, Australia will be more successful in pursuing its own defence agenda.

Currently, an extended, multi-tiered process is required for Australian entities to obtain US export licenses for transfers of defence articles. Although the US State Department's Directorate of Defense Trade Controls (the "Directorate") strives to reduce the review periods, its efforts do not address the learning curves, documentation, negotiations and administrative burdens required in seeking Directorate approval. These burdens not only interfere with Australia's access to needed technology, but risk causing unnecessary delay in Australia's response to US requests for support. Rapid deployment has become essential in the context of increasingly asymmetric and widely dispersed conflicts, where short notice is the trend. Allies cannot integrate

---

(settlement of such charges included a US$15 million penalty, see *In the Matter of The Boeing Company*, Consent Agreement, 28 March 2006, <http://www.pmddtc.state.gov/Consent%20Agreements/2006/The%20Boeing%20Company/Consent%20Agreement.pdf> [Accessed 6 June 2007]) and the ITT Corporation's unauthorized exports of night vision technology discussed below.

[5] Andrew Chutter, 'Report: Export Rules Don't Stop Tech Spread,' *DefenseNews*, 24 April 2006, p. 6, noting that a joint body convened by the Pentagon's Defense Science Board and Britain's Defence Scientific Advisory Council, delivered in March 2006 had observed that commercial off-the-shelf technologies place "very effective and militarily significant tools at the disposal of our adversaries" and gave as examples, WiFi, Bluetooth wireless networking technologies, public-key encryption, the Internet, hand-held GPS receivers and satellite imagery that enable terrorists and rogue states to set up robust, global command-and-control networks at insignificant costs, and that such advances will continue to become available at lower costs to such adversaries.

their forces unless such forces are properly equipped for interoperation. Unfortunately, regulations are often drafted without a full appreciation of the military exigencies. As noted by Air Chief Marshal Angus Houston, "The brevity of warning time almost ensures that we will join the fight with a 'come as you are' force."[6]

Australia's *Defence Capability Plan* suggests significant dependence on offshore procurement. A significant portion of this is expressly earmarked for US technology.[7] The difficulty with all offshore procurement from the US is that it must contend with ITAR and with other applicable US export control regulations. To the extent that misunderstandings of ITAR exist in the Australian defence community, ITAR compliance obligations will become a significant obstacle to effective Australian-US military interoperation. And to the extent the US perceives that Australian export controls fall short of ITAR, the US—in order to limit the risk of losing control of the end-uses of US military technology[8]—will resist requests for tech transfers, deny requests for access to the most advanced and sensitive data, or include onerous restrictions in those approved.

This will create substantial and costly compliance burdens for Australian recipients. As a first step in explaining how Australia might minimize such burdens, we now address some common misunderstandings of ITAR.

Fundamental Difficulties Concerning ITAR

US allies commonly underestimate ITAR, fostering institutional antagonism toward compliance, the creation of deficient controls that increase the inter-country friction and regulatory inertia, and further delaying and impeding the transfer of defence equipment and related technical data.

ITAR'S EXTREMELY BROAD SCOPE

Because ITAR has an unusually broad reach, it contains requirements that have no comparable counterpart (either in substance or in scope) in allied regulatory regimes. These are often overlooked or underestimated by potential purchasers. Misunderstandings of the scope of ITAR controls cause personnel to misdirect their efforts, seeking concessions rather than

[6] Air Chief Marshal Angus Houston, *Speech to RUSI Conference*, 16 May 2007, <http://www.defence.gov.au/media/SpeechTpl.cfm?CurrentId=6652>.

[7] For example, AIR 6000, the New Aerospace Combat Capability, specifies the JSF produced by Lockheed Martin. Since the LAND 53, NINOX – Night Fighting Equipment Replacement – identifies no significant possibility for Australian industry to contribute to the design of the equipment, it points to possible procurement from US manufacturers. See Australian Department of Defence, *Defence Capability Plan: 2006 – 2016*, Public Version, p. 31 and 105, respectively, accessed at <http://www.defence.gov.au/dmo/id/dcp/DCP_2006_16.pdf>.

[8] Space constraints preclude a discussion of "end use" certificates, i.e., what the ITAR refer to as DSP-83 *Nontransfer and Use Certificates*, but failure to abide by the terms and conditions of such certificates is another way that sensitive military technology slips out of control and prompts justifiable US concerns.

addressing the underlying US security concerns. The latter concerns can be addressed relatively cost- and time-effectively by implementing controls that are substantially equivalent to those required by ITAR. In the absence of such analogous controls, US counterparts will likely perceive a substantial risk that tech transfers to Australia could result in unauthorized releases to potential US adversaries.[9]

EXTENSIVE, RIGOROUS MEASURES REQUIRED TO ENSURE COMPLIANCE

ITAR requires exporters (and recipients of exports) to take unusually stringent measures to ensure compliance with ITAR's complex requirements.[10] A review of the ITAR conditions for authorized exports is helpful in determining what measures are necessary for export control compliance. For example, export approval by the Directorate is not required simply for transfers of military articles from the US to another country. Rather, any release of ITAR-controlled technical data, and any provision of defence services, requires separate approval by the Directorate. If a company in possession of such data does not maintain an up-to-date inventory of such data or does not supervise and control the movement of that data, it can discover belatedly that it has released it unintentionally or inadvertently in telephone conversations, face-to-face meetings, or even mouse clicks transmitting emails with tech data attachments. If Australian recipients do not maintain similar controls, they too are in violation of ITAR.

REMEDIAL ACTION EXPECTED UPON DISCOVERY OF ACTUAL OR SUSPECTED VIOLATIONS

ITAR strongly recommends (but does not require) that parties promptly and voluntarily self-report their actual and suspected ITAR violations. As a result, the US government has a high expectation for the remedial conduct that parties should undertake to avoid compounding violations. If a violator falls short in such remedial action, it risks turning civil noncompliance into criminal misconduct (punishable by heavy fines assessed against the company and by fines and imprisonment of culpable individuals).

ITAR Focuses on Control

It is helpful to understand the underlying policy rationale of ITAR. ITAR is first and foremost about preventing unauthorized dissemination of military technology. To this end, ITAR is designed to ensure *control* of items (defence articles, services, and related technical data) that, if not controlled,

[9] Such releases will be charged back to the US party under ITAR. As the ITAR Part on "Violations and Penalties" emphasizes: "Any person who is granted a license … *is responsible for the acts of* … all authorized persons to whom possession of the licensed defense article or technical data has been entrusted regarding the operation, use, possession, transportation, and handling of such defense articles or technical data *abroad*." 22 Code of Federal Regulations (CFR) §127.1(b). [Emphases added.]

[10] It must be remembered that ITAR imposes strict liability for violations, and the government need not prove intention to violate in order to establish an ITAR violation.

would jeopardize US national security and the security of US allies. In most countries, export control laws apply to the movement of goods across physical borders. But ITAR covers a host of intangibles as well as tangibles. And it does this in several layers. Like comparable export regimes, ITAR controls the taking or sending of defence articles out of the United States—that is, their physical transport. But it also controls taking or sending "*in any manner*." This includes transfer or release by mouse-click to an unauthorized party, or by placing such data on a web site that can be accessed from anywhere outside the US. It also includes "[d]isclosing (*including oral or visual disclosure*) or transferring technical data to a foreign person, whether in the United States or abroad,"[11] and treats as a "deemed export" any instance in which a foreign national gains access. The language applies with equal force to intangible transfers through digital media or the Internet. All "exports" of controlled articles and technical data must be expressly approved by the Directorate.

Moreover, ITAR defines "export" to include: "performing a defense service on behalf of, or for the benefit of a foreign person, whether in the US or abroad." Just as the ITAR-controlled article or data need never leave the United States in order for it to have been "exported," the ITAR-controlled defence service need not be performed outside the US for it to have been "exported." The imputed "transfer"/"export" can occur wholly within the US, if an unauthorized (i.e., foreign) person is involved. A "deemed export" is considered to have been made to the foreign national's home country, once he or she has received such data by reading, viewing or listening to it (regardless of where this occurs).

Any such transfer in the absence of a license from the Directorate constitutes a violation of ITAR. If done wilfully, it is a criminal offence. If a Silicon Valley company's Palo Alto office manager, for example, sends an email containing ITAR-controlled data to five employees who are US citizens or permanent residents, and one of them forwards it to another employee who is a foreign national (and not a US citizen or permanent resident), and does so without a license, the company has just "exported" that data in violation of ITAR. It would also constitute a violation if a comparable release, to someone who was not an Australian national, occurred within one of Adelaide's high tech companies.

What Kinds of Items Do ITAR's Controls Apply To?

ITAR controls a broad range of specialized goods termed collectively "defense articles." These include any "item or technical data" that the US government unilaterally elects to designate as such. Many (but not all) such designations appear in the "US Munitions List"—a misnomer in that most of the items on that list are not "munitions." This creates problems for both US

[11] 22 CFR §120.17. [Emphasis added.]

and non-US persons: almost everyone recognizes a tank or fighter jet as a "defense article" (even though neither is a "munition"), but the defence use of many seemingly non-defence-related items that are listed is hardly self-evident.[12]

A second highly misleading feature of the "Munitions List" is that it does not define the ambit of ITAR controls which, naturally, have been drafted to control export and import of all "defense articles." If ITAR controls were limited to specified items on the "Munitions List," any US adversary could simply monitor changes to the list to know, well in advance of deployment, when US companies were engaged in the development of new technologies.

What is less obvious to US allies is that ITAR also controls all "technical data" related to any "defense article." ITAR defines "technical data" with extraordinary breadth to include

(i) any and all "information" required for the design, development, production, manufacture, and assembly of defence articles;

(ii) "information required" for operation, repair, testing, maintenance or modification of "defense articles;" and finally

(iii) "classified information relating to defense articles and defense services."

To complicate the picture further, the definition of "defense services" includes the self-evident—

> furnishing of assistance (including training) to foreign persons, whether in the US or abroad in the design, development, engineering, manufacturing, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles

—but it is not limited to this. Somewhat surprisingly, "defense services" also contemplates "the furnishing to foreign persons of any technical data controlled" under ITAR, whether the data is in the US, Australia or anywhere else in the world. Virtually any technical data related in any way to a defence article is ITAR-controlled. If an Australian entity receives such data, it must control it in strict compliance with ITAR, which includes a prohibition on "re-export" unless expressly approved by the Directorate.[13]

[12] For example: a GPS system, "metal fuels in particle form," certain oxidizers, superfine iron oxide, atmosphere diving suits, tape recorders and cameras qualified to operate in outer space, safety glasses designed to protect against industrial accidents such as a thermal flash, navigation equipment, electronic security surveillance systems.

[13] 22 CFR § 124.8.

Easily Overlooked But Important Requirements

There are several frequently overlooked ITAR requirements. The easiest way to identify these is to compare the ITAR requirements to the technical data requirements of Allied countries. Some of the most important non-congruences include:

(i) no conditions attached to export licenses to limit their scope and application;

(ii) no Technical Assistance Agreements (TAA) to regulate tech transfers and services to persons outside the technology's country of origin; and

(iii) no rules to regulate release of technical data in digital media.

The US requires these to retain control over exported defence articles, services, and technical data. If the Australian defence community and policy makers want to maximize Australian access to US technology, they might consider instituting comparable arrangements.

US Export Licenses Are Not Omnibus Grants of Unlimited Use

Recipients far too often assume that upon delivery all ITAR-controlled articles, services and technical data "belong" to them: they are theirs to keep and to use in any manner they choose. This would defeat the ITAR policy intent of preserving the US military technological edge. An export license is thus expressly limited in scope, use, and duration. The ITAR requires that the license holder only export that quantity expressly authorized by the license. And all licenses issued by the Directorate "must be returned" to the Directorate "when the total value or quantity authorized has been shipped or when the date of expiration is reached, whichever occurs first."[14] By requiring return of the license, the ITAR reinforces an on-going obligation on the part of the recipient to retain control of the licensed article. A license to export ITAR-controlled defence articles is not transferable or renewable, nor can the recipient expect to amend it in order to export more than the authorized quantity. On the contrary, the ITAR goes so far as to declare a policy of denying all requested amendments for: "Additional quantity, changes in commodity, country of ultimate destination, end-use or end-user, foreign consignee and/or extension or duration."[15] Any such change requires that the approval process be repeated and a new license obtained.

Most important, most licenses come with multiple, tightly drawn conditions. Approval to export a submarine fire control system, for example, under a

[14] 22 CFR §123.22 (c).
[15] 22 CFR §123.25(c).

direct commercial sale agreement (not a government-to-government Foreign Military Sale) may contain restrictions against any

(i) export of US Navy blueprints,

(ii) release of technical data beyond the contractor's own "built-to-print" engineering drawings, and/or

(iii) release of tactical software "without prior permission" from the Directorate.

Such restrictions can put the US contractor in technical breach of its agreement with the Australian customer. As a result, before "exporting" such software, the US person must apply for a review of the software and the Directorate (on advice from other US agencies such as the US Navy) may decide, under circumstances then prevailing, to deny release of the code needed for the system to operate as desired or to fulfil certain key specification requirements.

License restrictions may also create an incentive for the US contractor to circumvent ITAR. In the example given, the contractor might think it can comply by removing the "US Navy" label from blueprints, providing explanations and technical data over the telephone to supplement drawings, or by releasing tactical software modules with unrestricted software in the hopes of obtaining later approval. It may not even seek such approval in the belief that the Directorate lacks the manpower to track such minutia among thousands of licenses granted annually. Such conduct does not benefit the Australian recipient and imperils the Australian defence community's relation with its US counterparts. The mere suggestion of association with a seller's circumvention or wilful violation of the ITAR invites Congressional inquiry and/or reference in Justice Department press releases. It can also prompt the US government to delay approval of important defence exports, bar an ally's military from access to sensitive data (despite a right of access under a government-to-government agreement),[16] or create an atmosphere of mistrust that can jeopardize tech transfer negotiations.

In addition, the cost of contravention is too often overlooked or only belatedly recognized as prohibitively high. The lesson here is simple: the Australian party to any contract for purchase of ITAR-controlled articles, services, or technical data should insist on reviewing (with competent US counsel) any application for an export license and any license issued in response, with particular attention to the attached restrictions. Doing so positions that party to avert any suggestion of complicity with the seller's advertent or inadvertent non-compliance. It also alerts the Australian party to the rigorous controls that such licenses customarily impose on recipients. This

[16] This happened with one customer ally for the Joint Strike Fighter.

is particularly important because such licenses uniformly *prohibit "re-export"* of the defence articles and technical data without prior permission of the Directorate. "Re-export" is another counter-intuitive and extremely broad concept that sweeps within its meaning not only advertent and inadvertent transfers, but also intra-company dissemination to unauthorized personnel (such as foreign nationals).[17] And, unlike "dual use" items,[18] ITAR-controlled items *are never licensed for "re-export" by the recipient*. Any re-export requires independent approval by the Directorate. It is therefore imperative that the purchaser understand the full scope of what is meant by a "re-export" under ITAR, and that it have a data governance program in place specifically tailored to avert inadvertent re-export.

RENDERING DEFENCE SERVICES OR RELEASING TECHNICAL DATA REQUIRES BOTH A LICENSE AND A TECHNICAL ASSISTANCE AGREEMENT

It is common sense to assume that issuance of a license to export a defence article (such as night-vision goggles or a GPS-chip for a cruise missile system) necessarily grants permission for the US contractor to perform services related to that equipment (such as explaining how to assemble, maintain and repair) and to release any technical data relevant to its proper use. If you bought a blender, you would expect to receive an operator's manual. A fighter plane is exponentially more difficult to operate and maintain properly and the risks from improper operation or maintenance are commensurately greater. But a license to export an ITAR-controlled defence article does not automatically grant permission to export the services and technical data necessary to train the purchaser to maintain and repair it. Because modern military equipment involves bundling hybrid technologies with multiple military end-uses, an inclusive authorization to export services for omnibus training would reveal all the related technical data, thereby imperiling the effectiveness of a weapon system by facilitating development of effective countermeasures. Hence the ITAR impose tight controls over both what data/tech support is transferred, and when and to what extent US persons may describe how to assemble, maintain, or repair the article.

The ITAR maintains control by sweeping activities related to the sensitive technology within the definitions of "export" and "defense article or service." Here "export" includes the performing of a defence service on behalf of, or for the benefit of, a foreign person, *whether in the United States or abroad*, and the ITAR defines "defense service" to include "furnishing to foreign persons of any" ITAR-controlled technical data.[19] "Technical data" also

[17] Notwithstanding recent concessions by the US to Australia and Canada on this subject, the ITAR continues to require in most instances that "re-exports" of defence articles, services and technical data not be made to foreign nationals within the recipient's country.

[18] Export of "dual-use" technologies are controlled by the Export Administration Regulations, administered by the US Commerce Department.

[19] 22 CFR §120.09 (a)(2).

includes "software … related to defense articles."[20] When we consider how much software is routinely required to operate, maintain, repair and update the bundled technologies of modern military equipment, the breadth of this restriction begins to become apparent. In addition, the terms "defense article" and "defense service" also include the modification of a commercial article for military use.[21]

ITAR also requires the parties to negotiate an appropriately inclusive Technical Assistance Agreement (TAA) in connection with the provision of services, including the release of any technical data. This document is essential if the purchaser is to gain effective use of defence articles it has purchased. Each TAA must contain certain required, non-negotiable provisions, some of which must be included verbatim.[22] The Directorate must review and approve all TAAs before they enter into force, and any such agreement must include Directorate approval as a condition to effectiveness. Any material amendment to such agreements must *also* receive Directorate approval. The following activities frequently require TAAs:

- Marketing products to foreign powers;
- Supporting sales to foreign parties;
- Providing overseas maintenance or training support;
- Technical studies or evaluations with foreign parties;
- Supporting a Foreign Military Sales case.

The TAA thus cannot be casually drafted. Directorate approval will apply *only* to those technologies and services specifically referenced in it. Failure to mention any necessary technical data will result in an under-inclusive TAA, potential for violation of ITAR, and further delays. It is essential that purchasers mentally map out everything they believe they will need in order to use purchased articles, services and technical data effectively *before* negotiating the TAA. This is where counsel in this field can be used cost-effectively to provide checklist review and to structure compliance programs. Like any other regulatory regime, ITAR has an internal logic that can be systematized to reduce compliance time and energy to a minimum, such that it does not impede use or deployment. If the Directorate is made familiar with an "Australian" compliance model, this could potentially cut review time and actually facilitate tech transfers under a kind of "most-favoured nation" logic (one based on an "approximately ITAR-compliant" model). Without

[20] 22 CFR §120.10 (a)(4).
[21] 22 CFR §120.3 (a).
[22] If such services, know-how, or data is in furtherance of the manufacturing of the defence article, a different agreement is required – a Manufacturing License Agreement.

systematic drafting and review, an under-inclusive TAA could result in the omission of vital technical data, failure to obtain authorization and the need for a time-consuming and costly formal amendment (with the concomitant secondary delay for Directorate approval).

While much of the text of the TAA is statutorily prescribed, it is hardly "boilerplate" and must be thoroughly vetted, because it imposes extraordinary requirements on the recipient of ITAR-controlled technology. One such required provision states:

> This agreement is subject to all United States laws and regulations relating to exports and to all administrative acts of the US Government pursuant to such laws.

By signing a TAA containing that language (as all do), the signatory has voluntarily acceded to extraterritorial application of all export-related US laws and cannot later credibly argue that this was never intended. Critically, this provision extends well beyond the ITAR, and includes, for example, the Export Administration Regulations (which control "dual use" items) and the Treasury Department's trade sanctions regulations.

Another required provision prohibits transfer of data to any "person in a third country or to a national of a third country." We once again encounter the "deemed export" concept, which controls transfers to foreign nationals in the US and in the recipient's country. Again, recall that the ITAR aims at retaining end-use control, and does so by requiring that the recipient maintain an array of procedures to protect against any unauthorized access. This is a zero tolerance universe. Not surprisingly, if an ally can demonstrate that it requires a comparable level of controls, the US will be more inclined to grant export of the desired defence article, service, or technical data.

In instituting comparable controls, US allies need not require each contracting party to reinvent the wheel: Systematic, routinized and uniform (across the national industry) compliance is the most cost- and time-effective approach to ITAR. It reduces the potential risk of violation, facilitates transfers, formalizes the terms of TAAs to make supervision more efficacious, and goes a long way to achieving the ultimate goal of approval. The industry itself can generate cross-industry standards, both for procurement and for compliance, that will streamline the process while effectively marshalling Australia's unique concerns so that they can be addressed uniformly by US parties and, thereby, provide significant negotiating leverage for Australian purchasing parties.

THE ITAR CONTROLS EXPORTS OF INTANGIBLES

Although the ITAR contains no express reference to digital data, the Internet, e-mail or any other digital enhancement of commercial communication, release of ITAR-controlled data on or through such digital media to a non-US

person clearly constitutes an "export" requiring US government approval. Of all the ITAR requirements that do not have comparable Allied counterparts, this is probably the one that creates the greatest risk of loss of control. Sensitive technical data in digital form flows like quicksilver. It easily escapes a company's control measures, particularly if those are not rigorous or are subject to lax enforcement:

> Data leaks persist because companies fail to focus sufficiently on controlling their data and averting ways in which they often lose control of it (for example, the unintended forwarding of email with attached files).[23]

The ITAR takes such risks far more seriously than do the export controls enacted by US allies (which tend either to leave intangible exports unregulated, or to apply ineffective large-mesh controls).

> As a result, nationals from Norway or the U.K. can make disclosures to US persons, consistent with their defense export controls, but reciprocal disclosures by US persons under similar circumstances (or in the same meeting) may be prohibited by the ITAR.[24]

This lack of congruence is particularly troublesome, because

> technical personnel engaged in problem solving meetings may exchange information or expertise, may provide technical advisory services, or may make proposals that are not primarily focused on observing the strict limits of the ITAR.[25]

Unless Australia tightens its controls of intangible transfers, it can expect the US to be reluctant to release highly sensitive technical data to Australian recipients, or to set burdensome conditions for its export. Australian entities that hope to be approved recipients of ITAR-controlled data will, therefore, need to implement an internal data governance plan tailored to the concerns of ITAR.

Lessons From The Current Enforcement Climate: *ITT Corp.'s Night Vision Division* Case

A recent case involving ITT Corp.'s Night Vision Division (ITT NV) illustrates what can happen to companies trying to circumvent the ITAR, and demonstrates the US government's attitude towards serious violations. It also reflects the government's expectation that companies will take measures consistent with national security when they discover or suspect an ITAR violation: that the offending company will move swiftly to report such violations, terminate all such activities, diligently attempt to recover illegally

[23] Roland Trope, 'Immaterial Transfers With Material Consequences', *IEEE Security & Privacy* (September/October 2006), p. 64.
[24] Roland Trope and Gregory Upchurch, *Checkpoints in Cyberspace: Best Practices for Averting Liability in Cross-Border Transactions*, American Bar Association, 2005, p. 238.
[25] Ibid.

exported articles and technical data, and tighten ITAR compliance and related training throughout the enterprise to avoid a reoccurrence. ITT NV's failure to pursue such a course of action resulted in it becoming the first major US defence contractor to be convicted of a criminal violation of the ITAR.[26]

ITT NV'S FALSE AND MISLEADING STATEMENTS

ITT NV produced night vision equipment, a technology critical to the US military capability, yet throughout the 1980s and 1990s, ITT NV failed to implement any ITAR compliance program.[27] Moreover, it routinely *temporarily* loaned or consigned ITAR-controlled night vision equipment to foreign customers for evaluation, under temporary foreign consignment agreements. Conditions in the export license for each such consignment required return of the equipment to the US prior to expiration.[28] Throughout the 1990's, ITT NV failed to comply with this requirement; and, as a direct result, it "lost track of numerous pieces of state-of-the-art night vision equipment."[29]

ITT NV did not promptly report the loss of such equipment. Instead, it sent the Directorate a "Preliminary Notification of Voluntary Disclosure", in April of 2000, stating that it "*recently discovered* apparent violations of the ITAR that involve ITT's loans and consignments of night vision equipment to foreign persons."[30]

Lawyers for the company asked the Directorate to consider as a mitigating factor that "*[u]pon realizing that it had a compliance issue with respect to these temporary exports, ITT took corrective action …*"[31] ITT NV sought "to

[26] US Department of Justice, Press Release: *ITT Corporation to Pay $100 Million Penalty and Plead Guilty to Illegally Exporting Secret Military Data Overseas*, 27 March 2007, <http://www.usdoj.gov/opa/pr/2007/March/07_nsd_192.html> [Accessed 6 June 2007]. The account presented here of the ITT NV case relies chiefly on the Appendix A "Statement of Facts" attachment to the Deferred Prosecution Agreement (signed by the US government and ITT), because ITT expressly agreed that such Statement "is true and accurate to the best of its knowledge and belief and establishes an adequate factual basis for ITT's plea" of guilty to the two criminal counts. *United States of America v. ITT Corporation*, Deferred Prosecution Agreement, "Factual Proffer," ¶5, p. 3. That Agreement and other relevant documents were accessible in March and April 2007 through the Department of Justice (DoJ) web site at <http://www.usdoj.gov/opa/pr/2007/March/07_nsd_192.html>. However, the DoJ subsequently terminated the links to these documents without explanation. The account is nonetheless based on copies downloaded from that web page prior to the termination of those links. A complete set of these documents can now be accessed at <http://www.roanoke.com/news/0327_agreement.pdf>, part of the web site maintained by *The Roanoke Times*, a newspaper in the state of Virginia.

[27] *United States of America v. ITT Corporation*, Deferred Prosecution Agreement, Appendix A, "Statement of Facts," p. 2.

[28] Note: all licenses are issued for four-year periods. 22 CFR §123.21 (a).

[29] Ibid, p. 3.

[30] Ibid, p. 4. [Emphasis added.]

[31] Ibid, p. 4. [Emphasis added.]

create the impression in the minds of the decision makers within the US Department of State that ITT 'recently discovered'" these violations, and had immediately taken swift corrective action.[32]

These representations were clearly false and misleading, and had two serious ramifications:[33] *first*, ITT NV would be liable for misrepresentations were the truth disclosed; and *second*, in spite of its awareness of the problem, ITT NV allowed risk to national security to continue unremedied. In the short term, ITT NV benefited. The Directorate required ITT to pay a US$8 million penalty, but ITT avoided a potential criminal conviction.[34] Subsequent investigation by the US government established that

> counsel for ITT Defense and the outside attorneys intentionally withheld material facts, information and circumstances about the consignment violations from the US Department of State[35]

ITT NV employees and managers had been aware of significant violations "since at least the mid-1990's." By March of 1998, more than two years before its April 2000 letter, ITT NV personnel had compiled a detailed list of "PAST DUE CONSIGNMENT EQUIPMENT."[36] When representing itself as making a "voluntary self-disclosure," however, ITT NV did not comply with the ITAR requirement to notify the Directorate "as soon as possible after violation(s) are discovered" and before conducting a thorough review.[37] Moreover, contrary to its representation of swift corrective actions, "few, if any, of the corrective actions set forth" in ITT NV's letter to the Directorate took place contemporaneously with its actual discovery of violations.[38]

EXPORT VIOLATIONS RELATED TO A SINGAPORE COMPANY

Among allies, it is usually prudent for dissatisfactions to be communicated privately. Public disclosure can exacerbate the immediate situation and threaten the long-term relationship. However, ITAR violations, particularly when they involve criminal conduct, cannot be kept under seal. The requisite debarment must be published in the Federal Register. Such public disclosure provides a compelling rationale for ITAR compliance by recipients

---

[32] Ibid, p. 5.

[33] Ibid, p. 4, noting a copy of the first letter "was also sent to corporate counsel for ITT Defense."

[34] Conviction of a criminal violation of ITAR requires a debarment from future export licenses.

[35] Ibid, p. 6.

[36] Ibid, p. 7.

[37] 22 CFR § 127.12 (c)(1). Although it must seem counter-intuitive to have a legal duty to report *prior* to investigating, that is nonetheless the ITAR regime. The rationale for this is clear. Because the penalties are severe and mitigations very limited under ITAR, the Directorate does not want to create time or incentive for violators to "spin" their account or conceal violations. ITAR's aim is to prompt disclosure in order to expedite recovery of misdirected sensitive equipment and technology.

[38] *United States of America v. ITT Corporation*, Deferred Prosecution Agreement, Appendix A, "Statement of Facts," p. 9.

of ITAR-controlled defence articles, services, and technical data. The potential risk to international standing can be seen in ITT NV's violations involving a Singaporean company.

Since the 1980's, ITT NV has purchased almost all its night vision optical assemblies from a Singapore company (Singapore Company). For that purpose, ITT NV routinely provided the Singapore Company with ITAR-controlled specifications and drawings for US military night vision goggles. Engineers from the two companies routinely worked together on optical and mechanical designs. In order to make such technical data transfers legally, ITT NV was required to obtain an export license from the US State Department. However, until 24 October 1994, ITT NV failed to obtain *any* export license to authorize the transfers to the Singapore Company. From 1994 to 1999, ITT NV obtained three limited-purpose export licenses authorizing transfer of a list of specifically identified ITAR-controlled drawings to the Singapore Company. However, ITT NV falsely represented such export as a "completely new shipment," where, in fact, it had already illegally transferred many of the same drawings.[39]

ITT NV committed additional violations by continuing to transfer ITAR-controlled technical data not covered by any of the three limited export licenses. The licenses contain a proviso that ITT NV could only export "build-to-print" technical data, and could not release any information which "discloses design methodology, engineering analysis, detailed process information or manufacturing know-how" to a non-US person. But ITT NV's engineers exceeded this limited "build-to-print" relationship in numerous collaborative discussions.[40]

By early 2000, ITT NV decided to seek the Directorate's approval of a TAA to authorize sharing the information already released to the Singapore Company during the previous 20 years. At that time, ITT NV elected not to disclose these violations, but left the government to uncover them during its criminal investigation.[41] In preparing its draft TAA, ITT NV created a TAA Annex that listed only drawings limited to a "build-to-print" type relationship.[42] The Directorate approved the TAA, with the following provisos:

> Proviso 5. Shipment of hardware against this agreement … *is not authorized* … [and] may take place only after the Department of State approves an amendment to the agreement.
>
> Proviso 6. Manufacturing technology, systems optimization/integration know-how, or design know-how *must not be released*.

[39] Ibid, p. 10.
[40] Ibid, p. 11.
[41] Ibid, p. 12.
[42] Ibid, p. 14.

> Proviso 7. Production *not authorized* without an approved manufacturing license agreement.[43]

These added provisos were designed to:

> limit what ITT NV could do under the TAA because of the sensitive night vision lens technology involved *and in recognition that Singapore was a well known conduit for military technology being channeled to the Peoples' Republic of China, a prohibited destination.*[44]

In spite of the express language in the TAA, ITT NV continued to export ITAR-controlled drawings and specifications without authorization, and to engage in collaborative discussions outside the limits of the "build-to-print" relationship. It also violated the provisos by exporting hardware to the Singapore Company and by producing millions of dollars of product.

In a December 1, 2003 letter, ITT NV admitted to the Directorate that it had been producing for years in violation of TAA Proviso 7 ("Production *not authorized* …"). However, its letter stated that unless it was relieved of Proviso 7, ITT would not be able to supply night vision goggles to the US military. In view of the ongoing war and soldiers' need for night vision capability, the State Department removed Proviso 7.[45] It is reasonable to infer that ITT NV's its attempt to use the safety of US armed forces as leverage weighed heavily as an aggravating factor in establishing later penalties.

EXPORT VIOLATIONS RELATING TO THE "LIGHT INTERFERENCE FILTER"

On the battlefield, night vision goggles are vulnerable to laser weapons, which can damage, degrade or destroy them. To avoid leaving a pilot or soldier "night blind," the US military developed "light interference filters" (LIFs). The critical nature of LIF technology led the government to classify portions of the specifications as "Secret" and to give them the special designation "NOFORN." This designation means "it cannot be shared with any foreign country, even the closest military allies of the United States."[46] In 1999, the LIFs were manufactured by an ITT NV subcontractor in California (the "California Company"). To reduce its costs, ITT NV pressured the California Company to lower its prices, and the California Company responded by exploring the possibility of outsourcing production of the LIF's critical component, the substrate lens, to a company in the People's Republic of China (PRC). In July 1999, the California Company applied for an export license to send the drawing for the LIF substrate lens to a company in Shanghai. The Directorate rejected the application for reasons of "National Security," because ITAR identifies the PRC as a prohibited

[43] Ibid. [Emphasis added.]
[44] Ibid. [Emphasis added.]
[45] Ibid, p. 15.
[46] Ibid, p. 16.

destination.[47] ITT NV ultimately outsourced the work to the Singapore Company. In spite of and in direct disregard of the "NOFORN" classification, it faxed a drawing package for the LIF to the Singapore Company.[48] The Singapore Company used those drawings to prepare an ITAR-controlled derivative LIF drawing, and exported the ITAR-controlled derivative drawing to an optics company located in the PRC. The PRC company quickly began production of the LIF substrates, ultimately manufacturing thousands of the LIF substrate lenses illegally.[49] Many of those have never been recovered.[50]

EXPORT VIOLATIONS RELATING TO THE "ENHANCED" NIGHT VISION GOGGLE SYSTEM

In July 2000, the US Army awarded ITT NV a development contract for the next generation night vision technology—an enhanced night vision goggle system that would optically blend night vision with thermal imaging.[51] The following year, the Army requested prototypes of the enhanced night vision goggle system (ENVG) from several contractors, including ITT NV.[52] Without obtaining an export license, and in violation of ITAR, ITT NV began to work collaboratively with the Singapore Company on the design and development of an ENVG prototype. It shipped ITAR-controlled drawings to the Singapore Company, and brought one of the Singapore Company's engineers to the US to work on the project. When the US-based Singapore engineer departed, ITT NV outsourced his work to the Singapore Company. Without obtaining a license, ITT NV continued to transfer ITAR-controlled drawings and specifications for the ENVG.[53]

The team that performed the work at the Singapore Company included two optical designers who were citizens of the PRC. They routinely had access to the illegally released, ITAR-controlled drawings. In 2003, they returned to the PRC. According to an ITT NV optical engineer, ITT NV's violation of the ITAR in this instance harmed US interests because "[b]y knowing the optical train of the ENVG … they [the PRC engineers] can determine how the whole system works."[54] On February 27, 2004, without a license or TAA, ITT NV released to the Singapore Company "the most up-to-date" ITAR-controlled ENVG performance specifications.[55] It subsequently released an ITT specification and drawing for an ENVG beam combiner in order to obtain a manufacturing quote for "10,000/year for 2006 and beyond" from the

[47] Ibid, p. 18.
[48] Ibid, p. 20.
[49] Ibid, p. 21.
[50] Ibid, p. 27.
[51] Ibid.
[52] Ibid, pp. 27–28.
[53] Ibid, p. 29.
[54] Ibid.
[55] Ibid, p. 30.

Singapore Company[56] ITT NV attempted to conceal these transfers by referring to the equipment by an inaccurate description.[57]

ITT NV'S CONSENT TO GUILTY PLEA FOR CRIMINAL VIOLATIONS

Under its plea agreement, ITT agreed to pay US$100 million in criminal fines, penalties, and forfeitures. ITT also agreed to engage an independent monitor and staff who will report to the US government on ITT's compliance with the plea agreement.

LESSONS FROM THE ITT NV CASE

From an Australian policy maker's perspective, the ITT NV case is vexing. The US law assumes that continued access to US Government contracts worth tens of millions of dollars would provide a defence contractor with sufficient incentives to comply with the law. A government contract shields the US manufacturer from numerous market risks and offers it the substantial benefit of developing new military technology at government expense, the expertise from which can then be used to make products for profitable commercial use. These benefits apparently did not offer ITT NV a sufficient incentive to comply with the law. Clearly the strategic advantage of developing next generation military technology is dissipated or destroyed if the developer ignores ITAR and releases technical data indiscriminately.

Policy makers should appreciate the influence the ITT NV case will have on their US counterparts in future negotiations for highly sensitive tech transfers. US negotiators will probably test assurances of ITAR compliance to determine whether the risks of circumvention and indiscriminate release have been adequately addressed. Australian contractors might consider explicit assurances directed at the ITT NV-type risks. This is particularly apt for the JSF, where an important part of the justification for Australia's costly investment is its anticipated receipt of highly valuable tech transfers.[58] The ITT NV case will clearly affect all negotiations for such tech transfers in the foreseeable future, and should be addressed up front and explicitly to avoid wasteful delays. This could also have the collateral benefit of putting Australia in a position to be among the earliest recipients when certain technologies classified as "NOFORN" are re-classified for release to US allies.

A further lesson from the ITT NV case is clearly that failure to impose ITAR-quality controls on contractors interested in receiving ITAR-controlled tech transfers can inadvertently encourage violations of ITAR, and such violations will have an adverse affect on the purchasing country. Ultimately, the

[56] Ibid, pp. 32–33.

[57] Ibid, p. 33.

[58] It will, of course, be even more essential to consider such assurances in Australian programs such as LAND 53, NINOX – Night Fighting Equipment Replacement that would presumably seek to incorporate the latest enhancements in night vision systems.

Australian government needs to ensure that it has the power to limit the likelihood of such violations. The costs of compliance are far exceeded by the potential costs of damage to historical defence relationships.

Conclusion

To ignore ITAR's complexities is to negotiate for access to US technology at a serious disadvantage. It will facilitate such negotiations and the ultimate transfer of the desired technology if Australian policy makers appreciate the ITAR's "control" objective, its comprehensive scope, the rigor required for lawful compliance with its provisions, and its trans-Pacific reach (including bans on re-export and on unauthorized release of controlled technical data). The trust that Australian and US military personnel share is continuously earned and reinforced in operations, mission planning and intelligence sharing. It can only be strengthened by learning from the mistakes of the larger defence community. Moreover, mutual trust does not automatically translate into omnibus tech transfers. With this in mind, Australian parties should craft their requests to address US concerns so as facilitate these transfers. Efforts to obtain US concessions on "re-export" in Australia of ITAR-controlled technical data to foreign nationals should be given a lower priority than obtaining the desired tech transfers in the first instance, particularly in light of the fact that gaining a technological edge is an important justification for the equipment's purchase price.

The ITT NV case demonstrates the legitimacy of US concerns with respect to the diversion of highly sensitive technologies. It would probably be beneficial, therefore, for Australian policy makers to create a regulatory regime that mirrored the ITAR standard. This would facilitate understanding and trust, communication and negotiation, and finally transfer of needed technology. A simple approach to this would include: limiting the application of such regulations solely to those projects that will incorporate ITAR-controlled items; focusing on the growing risk of intangible transfers on digital media or through the Internet; considering whether there is sufficient emphasis on export compliance training at all levels of an enterprise; reviewing penalties for violation to determine whether they provide sufficient deterrence; and above all, recognizing that ITAR-control follows across borders—ITAR continues to apply even after the relevant defence article or technical data leaves the shores of the United States or enters the mind of an Australian citizen. The benefit from such scrutiny would almost certainly be an increased willingness on the part of US to approve sensitive tech transfers to an important ally.

Roland Trope is a partner in the New York City offices of the law firm of Trope and Schramm LLP, an Adjunct Professor in the Department of Law at the United States Military Academy at West Point, and an Associate Editor of the journal IEEE Security & Privacy. roland.trope@verizon.net.

Dr. Monique Witt is a lawyer in New York City. zevisgirl@yahoo.com.