



AUSTRALIAN INDUSTRY  
GROUP

**DEFENCE COUNCIL OF THE AUSTRALIAN INDUSTRY GROUP**

10 September 2010

PM/DDTC  
SA-1, 12th Floor  
Directorate of Defense Trade Controls  
Office of Defense Trade Controls Policy  
ATTN: Regulatory Change--Nationals  
Bureau of Political Military Affairs  
U.S. Department of State  
Washington, DC 20522-0112  
by email: [DDTCResponseTeam@state.gov](mailto:DDTCResponseTeam@state.gov)

ABN 76 369 958 788

Level 2  
44 Sydney Avenue  
FORREST ACT 2603  
PO Box 4986  
KINGSTON ACT 2604  
AUSTRALIA  
Telephone: 02 6233 0700  
Facsimile: 02 6233 0799  
[www.aigroup.asn.au](http://www.aigroup.asn.au)



Australian Industry Group  
Defence Council

**Comments on Proposed Rule, 75 Fed. Reg. 48,625-48,627 (Aug. 11, 2010) -  
Amendments to the International Traffic in Arms Regulations (ITAR) 22 C.F.R. Parts  
120-130: Dual Nationals and Third-Country Nationals Employed by Foreign End-Users  
and Consignees**

The Australian Industry Group Defence Council (Ai Group Defence Council) welcomes the opportunity to provide comment to United States Department of State on the proposed amendments to the International Traffic in Arms Regulations: Dual Nationals and Third-Country Nationals Employed by End-Users.

Ai Group Defence Council has provided the leading voice for Australia's defence industry since 1979. With over 100 member companies from prime to small contractors, whose activities cover the spectrum of defence business – from systems and platform development, systems integration, manufacture and through-life support and facilities construction through to providing base support and personnel services. Through Ai Group Defence Council leadership, our members demonstrate their commitment to best-practice export control principles.

Ai Group Defence Council welcomes the President's Task Force on Export Control Reform, which has recommended the current policy regarding the treatment of dual nationals and foreign nationals be reconsidered.

While the stated intent of the proposed amendments is to take a step forward on the dual/third country national issue, there are a number of areas associated with the proposed rule that we believe are ambiguous and may result in unintended consequences. In particular, though the stated intent of the amendment is to reduce the administrative burden on approved end-users, and eliminate the potential conflict with local laws on anti-discrimination, human rights, and the privacy of personal data privacy grounds, elements of the proposed rule may in fact exacerbate both.

Our detailed comments on the proposed amendments are as follows:

1. Screening:

- a. §126.18(b) requires the foreign recipient of a defense article, including technical data, to implement effective procedures to prevent unauthorised transfer or access to defense articles. Pursuant to §126.18(c), this can be demonstrated through either the proposed recipients employees' possession of Government approved security clearances or a process to screen employees (and a signed

non-disclosure agreement). There is no indication in the proposed amendment that these requirements are to be limited to dual/third country nationals as defined by the Department of State, so they could be construed as a general application. If interpreted as of general application, then in trying to address a specific issue, it is possible that the proposed rule will increase the administrative burden on foreign end-users and relevant Government agencies alike.

At present, there is no requirement for all employees who may have access to ITAR controlled articles to hold a Government security clearance. If this were to become a prerequisite, the provision and maintenance of such clearances would place a heavy administrative burden on both the Government agency and foreign end-user. Timescales to achieve security clearances can be protracted, and the provision of security clearances purely to achieve ITAR obligations is unlikely to be afforded a high priority by the issuing authority.

The alternative of a company-designed screening process could be quite burdensome because it would apply to all employees and there is no express guidance on the minimum standards that this screening process might take. This poses a real risk of inconsistent application, with serious consequences for those foreign end users who are deemed to not have achieved the expected 'standard'. It appears foreign end users will have to self-determine their own screening process and threshold for 'substantive contact', as well as when DDTC authorisations should be sought. This represents a risk that will be difficult for companies to manage and may drive a move towards ultra-conservative assessments that add to rather than provide administrative relief. Moreover, read in the context of §126.18(c)(2), there is a real risk that the human rights issue identified by DDTC would be exacerbated rather than resolved.

- b. §126.18(c)(2) requires that employees be screened for 'substantive contacts' with restricted or prohibited countries listed in §126.1. It is not clear whether this screening applies generally, or only to a subset of employees (either dual/third country nationals or only employees requiring access to ITAR controlled material). The screening process in §126.18(c)(2) could be read consistently with §126.18(c)(1) to only apply to those dual/third country nationals who do not have a security clearance, however, it needs some clarification to make that clear. Such a narrower screening process would be consistent with the stated intention for the proposed change.

Irrespective of application, the nature of the screening program (without further guidance as to minimum requirements) has the potential to become quite intrusive, exposing foreign entities to legal challenge under national privacy or human rights legislation (both in terms of the investigation and any decision-making process resulting from the investigation).

The requirements of §126.18(c)(2) are potentially more intrusive than current issues in respect of country of birth, etc. Presently, employees are screened for nationality, however the new change shifts the focus to include screening of an employee's private life, personal relations and activities. For example, what are the implications for an employee who is not a dual/third country national but who is married to a former national of a §126.1 country and regularly travels there for family visits? What about someone whose only ties to a §126.1 country is that their parents were nationals of that country, though the individual is not; or the marketing representative who travels regularly to a §126.1 country in pursuit of commercial business not related to ITAR.

Making screening records available to DDTC (or its agents) upon request could also prove to be problematic. If such records reveal personal data about individuals, making this information available to DDTC would continue to raise local human rights/privacy concerns, and lead to greater administrative and legal costs to foreign end-users.

Even if found to be legally acceptable, the need for a screening process for substantive contacts would pose a heavy administrative and bureaucratic burden on individual companies.

Practically, it would be impossible to expect a company to conduct employee surveillance so as to verify employee travel and confirm an employee's personal relationships whilst away from work. For example, the idea of having an employee sign a certificate may satisfy a lawyer that some due diligence was conducted, but in reality certificates stating that employees "have not..." are reactive, not pro-active measures, and do little to guarantee control of future behaviour.

- c. It would be preferable if the proposed amendment be clarified to only apply to such persons who require access to ITAR controlled material, and that a security clearance issued by a Government agency would, by itself, be prima facie evidence of compliance and sufficient due diligence, without further requirement to screen such individuals. This would allow the foreign end user to rely on the Government agency's screening procedures to satisfy compliance requirements, and would be within local legal boundaries.

In circumstances where an individual does not have a security clearance, but requires access to ITAR controlled material, any screening should be limited only to dual/third country nationals. No screening should be required for non-dual/third country nationals. That is, the proposed changes under the §126.18 exemption should not overturn the Australian exemption established in the licensing guidelines.

## 2. Bona fide Employees:

The proposed amendment specifies that transfers would be limited to dual nationals or third-country nationals "who are bona fide, regular employees, directly employed by" the end-user or consignee. It would therefore appear that contract employees, temporary workers, or consultants would not be included under the operation of the proposed rule § 126.18. It would be preferable if this was expressly addressed and permitted under the proposed rule.

## 3. § 124.16:

The authorization in §124.16 is proposed to be removed, presumably because it is no longer needed. Consideration should be given to retaining those provisions, possibly as an alternative to the proposed rule. With minor rewording, e.g. automatic application, it could be combined with the new §126.18 and provide a helpful structure to the management of the dual/third country national issue. As §124.16 already covers dual/third country nationals from the EU, NATO, etc, keeping it would leave the new §126.18 to apply to dual/third country nationals from non-§124.16 countries. Maintaining §124.16 would also be particularly helpful if the screening is going to be required for all employees, not just dual/third country nationals.

If it remains the intention that §124.16 be removed it would be helpful if a note was added in the ITAR to say that §124.16, if already used in an Agreement, shall remain in force for that Agreement until such Agreement is later amended to include the new §126.18.

## 4. Defense Services:

§126.18(a) appears to exempt only transfers of ITAR-controlled defense articles and technical data, but not defense services. By definition providing a defense article to a foreign person is a defense service, hence the §126.18(a) should be clarified to include defense services.

5. "End User" vs "Consignee":

There is some doubt as to how the various provisions of the proposals apply to "End Users" and "consignees" and the relationship between them. These proposals would greatly benefit from clarification before publication,

Thank you for consideration of our views.

A handwritten signature in black ink, appearing to be 'I. Willox', written over a horizontal line.

**INNES WILLOX**  
Executive Director