sipri

SIPRI Good Practice Guide
Export Control ICP Guidance Material

July 2017/No. 2

INTERNAL COMPLIANCE AND EXPORT CONTROL GUIDANCE DOCUMENTS FOR THE INFORMATION AND COMMUNICATIONS TECHNOLOGY SECTOR

SIBYLLE BAUER, KOLJA BROCKMANN, MARK BROMLEY AND GIOVANNA MALETTA

INTRODUCTION

This SIPRI Best Practice Guide outlines the sector-specific compliance-related guidance material that is available to companies and other actors in the information and communications technology (ICT) sector that might be subject to the European Union's arms and dual-use export controls.[1] It covers guidance material produced by national governments, the EU and other bodies, as well as publicly available Internal Compliance Programmes (ICPs) produced by companies in the ICT sector.

The ICT sector is significantly affected by dual-use export controls, particularly through the controls on cryptography, which is an integral part of many of the systems it produces. Cryptography is used to securely store or transfer information. For reasons of national security, systems that employ a certain standard of cryptography have been covered by the Wassenaar Arrangement's dual-use export control list since the 1990s. The impact of dual-use export controls on the ICT sector has recently been affected by the expansion at both the Wassenaar Arrangement and EU levels of controls on so-called cyber-surveillance technologies.[2] Additional EU-level controls are being considered in connection with the ongoing review of the EU's Dual-use Regulation (EC 428/2009).

Given this evolving landscape, there is a clear need to make companies and other actors in the ICT sector better aware of the compliance-related guidance material that is already available—particularly that related to controls on cryptography and cyber-surveillance technologies—and to fill any remaining gaps.

[1] For further information, see SIPRI, 'Challenges and good practices in the implementation of the EU's arms and dual-use export controls: A cross-sector analysis' (forthcoming).

[2] Cyber-surveillance technologies are widely used by law enforcement agencies (LEAs) and intelligence agencies. They enable the monitoring and exploitation of data or content that is stored, processed or transferred via ICT platforms and devices from computers to mobile phones and telecommunications networks.

SERIES SUMMARY

● The scope of European Union (EU) dual-use and arms export controls has expanded in recent years to cover a wider range of goods, technologies and activities. This means that a broader range of sectors and actors are now affected by controls. This expansion has been accompanied by efforts by governments and the EU to incentivize the adoption of internal compliance programmes (ICPs) by companies and other affected entities. An ICP is an arrangement that a company or other entity puts in place to ensure that it is complying with dual-use and arms export controls. However, while the requirement to have an ICP is becoming more mainstream, the guidance available on how one should be established and maintained is often generic and fails to take into account the specific needs of different affected sectors and actors. This SIPRI Good Practice Guide is one of a short series that helps fill this gap by collecting available sector or actor-specific compliance-related guidance material. This Guide presents guidance that is available to companies and other actors in the information and communications technology (ICT) sector. It covers guidance material produced by national governments, the EU and other bodies, industry associations as well as publicly available ICPs produced by companies and other actors in the ICT sector.

GOVERNMENT- AND EU-ISSUED GUIDANCE MATERIAL

Australian Government, Department of Defence, 'Australian export controls and ICT' (Apr. 2016), <http://www.defence.gov.au/exportcontrols/_Master/docs/Australian_Export_Controls_and_ICT.pdf>.

> This document provides guidance on where Australia's export controls apply to the ICT sector and explains how to apply for advice and for permits. It also discusses the circumstances in which an exporter is not required to apply for a permit and the general exemptions that exist. In addition, it outlines the main ICT items on Australia's defence and strategic goods lists and discusses record-keeping and reporting standards. The guide provides a number of case studies to help to determine whether a permit is required.

United Kingdom Department for Business Innovation and Skills, 'Intrusion software tools and export control' (Aug. 2015), <http://webarchive.nationalarchives.gov.uk/20160701131101/http://blogs.bis.gov.uk/exportcontrol/files/2015/08/Intrusion-Software-Tools-and-Export-Control1.pdf>.

> This note explains the UK Government's interpretation of the coverage of the controls on 'intrusion software' that were added to the Wassenaar Arrangement's dual-use list in 2013 and the EU's dual-use list in 2014. The note describes the rationale for and operation of both the intrusion software controls and export controls more generally. It also outlines the relevant types of export licences and general exemptions. Finally, the note discusses the specific control texts and provides practical examples of what might or might not be controlled.

European Commission, Institute for Human Rights and Business, and Shift, 'ICT sector guide on implementing the UN Guiding Principles on Business and Human Rights' (June 2013), <https://www.ihrb.org/pdf/eu-sector-guidance/EC-Guides/ICT/EC-Guide_ICT.pdf>.

> This guide advises companies in the European ICT sector on the steps they need to take in order to effectively implement the 2011 United Nations Guiding Principles on Business and Human Rights. Although not explicitly focused on arms and dual-use export controls, the report contains a large amount of relevant compliance-related guidance and advice, particularly in relation to risk assessments and supply chain management.

European Commission, Directorate-General Trade, 'FAQ on controls of "information security" items and implementation of the cryptography note exemption', Guidance Note (Oct. 2016), <http://trade.ec.europa.eu/doclib/docs/2016/october/tradoc_155052.pdf>.

> This note provides guidance for exporters in the ICT sector and, more specifically, on the application of the cryptography note exemption, which outlines the situations in which items are exempt from the controls on the export of items that contain cryptography. It also sets out good practices for interpreting the relevant provisions of the EU Dual-use Regulation in order to reduce divergences in their application.

Although agreed by all EU member states, the guidance is not binding and does not overrule rulings by national authorities or the European Court of Justice.

OTHER GUIDANCE MATERIAL

Cohn, C. and York, J., '"Know your customer" standards for sales of surveillance equipment', Electronic Frontier Foundation (Oct. 2011), <https://www.eff.org/deeplinks/2011/10/it%E2%80%99s-time-know-your-customer-standards-sales-surveillance-equipment>.

This report outlines a set of due diligence measures that companies engaged in the sale of surveillance equipment should perform. The report argues that companies should audit their current and potential customers for human rights abuses, and should get to know their customers before selling surveillance technology. They should also avoid sales where there is a risk their products might be used to violate human rights. Although not explicitly focused on arms and dual-use export controls, the report contains a large amount of relevant compliance-related guidance and advice, particularly in relation to risk assessments and supply chain management.

Information Technology Telecommunications and Electronics Association (techUK), 'Assessing cyber security export risks' (Nov. 2014), <https://www.techuk.org/images/CGP_Docs/Assessing_Cyber_Security_Export_Risks_website_FINAL_3.pdf>.

The aim of this guide is to help companies to 'identify and manage human rights and national security risks associated with the export of security cyber products and services'. The report is mostly focused on the export of cyber-surveillance and cybersecurity products that are not subject to export controls, but where there are security and human rights concerns that companies should take into account. The report provides 'background information on various human rights and national security risks' and outlines the types of due diligence standards that companies should apply.

Ericsson, 'ICT and human rights: An ecosystem approach' (Apr. 2013), <https://www.ericsson.com/res/thecompany/docs/corporate-responsibility/2012/human_rights0521_final_web.pdf>.

This document by the ICT company, Ericsson, sets out frameworks to guide businesses on human rights. The document proposes three strategies for companies confronted with human rights abuses: convincing the government to act differently, refusing to comply with requests in violation of human rights or pulling out of the specific market. Ericsson proposes a human rights corporate governance framework to cope with related ethical dilemmas, and adopting internal policies that are in line with UN human rights provisions and other internationally accepted standards.

Institute for Human Rights and Business, 'Human rights challenges for telecommunications vendors: Addressing the possible misuse of tele-

communications systems, Case study: Ericsson', Case Study no. 2 (Nov. 2014), <https://www.ihrb.org/pdf/2014-11-18_Digital-Dangers-Ericsson-Case-Study.pdf>.

This case study describes the challenges faced by ICT companies, such as Ericsson, in cases where their technology is misused by third parties in ways that infringe human rights. It makes 'key recommendations' for vendors of ICT on internal communication, escalation processes, awareness raising, risk assessment processes and contract specifications.

Anderson, C., 'Considerations on Wassenaar Arrangement Control List additions for surveillance technologies' (13 Mar. 2015), <https://s3.amazonaws.com/access.3cdn.net/f3e3f15691a3cc156a_e1m6b9vib.pdf>.

This report provides a detailed analysis of the controls on 'intrusion software' and 'IP Network surveillance systems' that were added to the Wassenaar Arrangement's dual-use list in 2013 and the EU's dual-use list in 2014. The report provides a technical analysis of the range of systems captured by the controls and examples of the kind of systems that might be captured by them.

SIPRI is an independent international institute dedicated to research into conflict, armaments, arms control and disarmament. Established in 1966, SIPRI provides data, analysis and recommendations, based on open sources, to policymakers, researchers, media and the interested public.

The research for the SIPRI Good Practice Guides on Export Control Internal Compliance Programme (ICP) Guidance Material was funded by the US State Department's Export Control and Related Border Security (EXBS) Program.

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE

Signalistgatan 9
SE-169 72 Solna, Sweden
Telephone: +46 8 655 97 00
Email: sipri@sipri.org
Internet: www.sipri.org