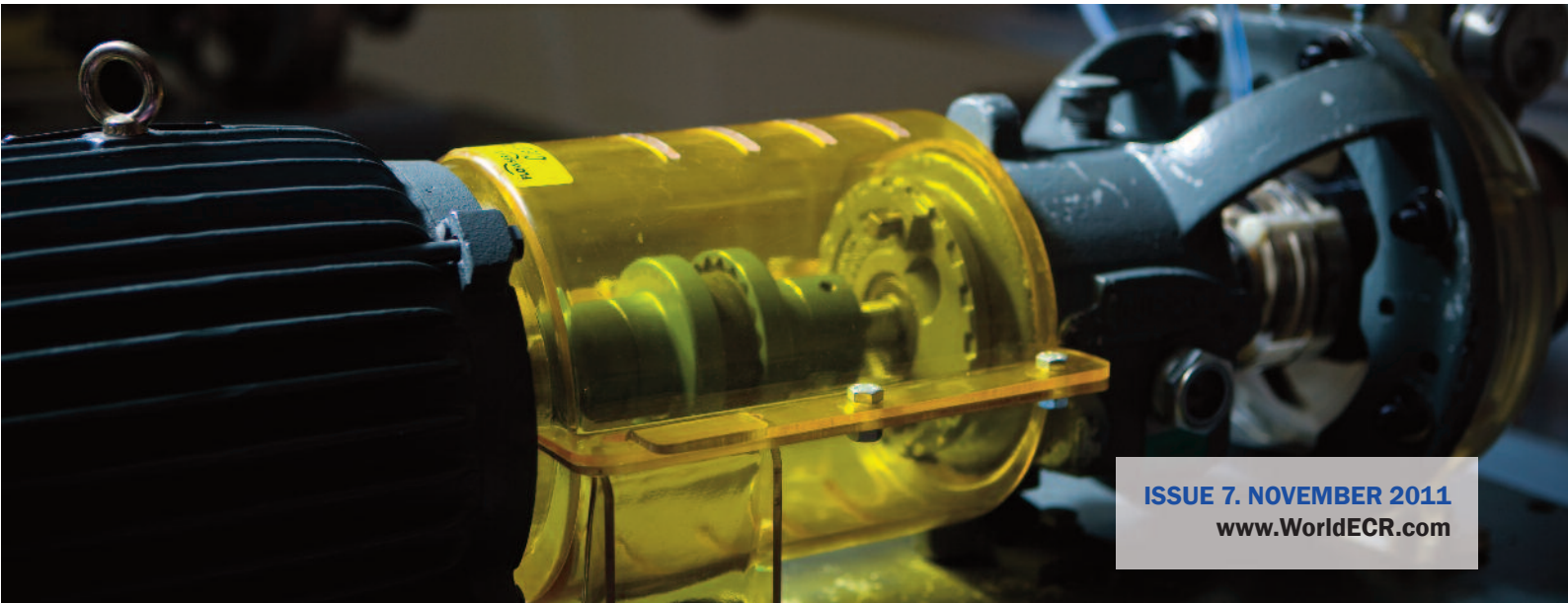
WorldECR



ISSUE 7. NOVEMBER 2011
www.WorldECR.com

Australia introduces defence trade bill

On 2 November, Australia's Minister for Defence Materiel, Jason Clare MP introduced the Defence Trade Controls Bill 2011 ('the Bill') to parliament along with the Customs Amendment (Military End-Use) Bill 2011, which is intended to support provisions within the Bill 'to strengthen export controls in line with international best practice'.

A key feature of the new legislation is that it implements the Australia-United States Defence Trade Cooperation Treaty (See *WorldECR* issue 5) which removes the requirement for individual licences to be obtained for each export, and allows for the licence-free movement of eligible defence articles within the approved Australian and U.S. communities.

Introducing the Bill, Clare said that around half of Australia's war-fighting assets are sourced from the United States, and that over the course of the next ten to 15 years, the country would be upgrading or replacing around 85% of its military equipment. Consequently, he said, 'Strengthening this area of our alliance cooperation is...clearly in our national interest.'

Currently, Australian companies that need access to defence items or technology from the United States must seek an export licence from the U.S. Department of State in accordance with the International Traffic in Arms Regulations ('ITAR').

Gaps in the system

In explanatory literature, the Australian government says that it had recognized that there were gaps in the country's existing defence export controls which could be categorized as pertaining to four areas:

- intangible transfer of technology;
- provision of services relating to defence and strategic goods and technology;
- brokering of supply of these goods, technology and related services; and
- exportation of goods intended for a military end-use that may prejudice Australia's security, defence or international relations.

Phillip Minnis

Bills introduced to the Australian parliament 'should 'strengthen export controls in line with best practice.'

By way of illustration, it notes that the existing export control regime has a focus on exports of physical goods, but that 'with the growth of technology, many defence export services can be provided over the internet or through brokers. These are not captured under the existing controls.'

Catch-all provision

In addition to the main legislation, proposed amendments to the Customs Act 1901 effectively introduce a 'catch-all provision' in the form of a new power to prohibit the export of 'non-regulated' goods that may contribute to a 'a military end use that may prejudice Australia's security, defence or international relations.'

However, the government says that it believes that this will be used in exceptional circumstances, and will have a 'negligible impact' on industry and trade.

Links and notes

The Defence Trade Controls Bill can be found at:
http://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r4700_first-reps/toc_pdf/11226b01.pdf;fileType%3Dapplication%2Fpdf

The Customs Act amendment is at:
http://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r4696_first-reps/toc_pdf/11224b01.pdf;fileType%3Dapplication%2Fpdf

Europe strengthens Burma sanctions

On 27 October, the European Commission announced the tightening of sanctions against Burma. The changes amend Regulation (EC) No. 194/2008. Key changes now read as follows:

Article 11

1. All funds and economic resources owned, held or controlled by the natural or legal persons, entities and bodies listed in Annex VI shall be frozen.
2. No funds or economic resources shall be made available, directly or indirectly, to or for the benefit of the natural or legal persons, entities or bodies listed in Annex VI.
3. The participation, knowingly and intentionally, in activities the object or effect of which is, directly or indirectly, to circumvent the measures referred to in paragraphs 1 and 2 shall be prohibited.
4. The prohibition set out in paragraph 2 shall not give rise to liability of any kind on the part of the natural or legal persons or entities concerned, if they did not know, and had no reasonable cause to suspect, that their actions would infringe this prohibition.

Annex VI is also amended so as to include 'senior members of the former State Peace and Development Council (SPDC), Burmese authorities in the tourism sector, senior members of the military, the Government or the security forces who formulate, implement or benefit from policies that impede Burma/ Myanmar's transition to democracy, and members of their families.'

Full details of the amendment at:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:281:0001:0002:EN:PDF

News and alerts

U.S. enforces anti-boycotting laws

The United States Bureau of Industry and Security ('BIS') announced settlements with a total value of $72,000 for alleged anti-boycotting law violations, at the end of October. The settlements were with four companies.

U.S. anti-boycott laws prohibit U.S. persons from acting with intent to comply with or support unsanctioned foreign boycotts. In the vast majority of cases, this means the boycott against Israel by the Arab League or other countries.

The settlements

Chemguard Inc. of Texas agreed to pay $22,000 to settle seven allegations that it violated the anti-boycott provisions of the EAR.

BIS alleged that, between 2005 and 2007 the company made seven violations, in connection with transactions involving the sale and/or transfer of goods or services (including information) from the United States to the United Arab Emirates. On two occasions, BIS says, the company furnished prohibited information in a statement regarding the blacklist status of the carrying vessel, and, on five occasions, failed to report the receipt of a request to engage in a restrictive trade practice or boycott, as required by the Export Administration Regulations ('EAR'), to the Department of Commerce .

The Shanghai-branch of the *Bank of New York Mellon* agreed to pay $30,000 to settle allegations that, in connection with transactions involving the sale and/or transfer of goods or services (including information) from the United States to United Arab Emirates, the bank 'furnished prohibited information in a statement certifying that the goods were neither of Israeli origin nor contained Israeli materials'. *World Kitchen LLC* of Pennsylvania, which, it is alleged, failed on five occasions to report to the Department of Commerce the receipt of a request to engage in a restrictive trade practice or boycott, in connection with transactions between the United States and the United Arab Emirates, will pay $10,000.

Tollgrade Communications, also of Pennsylvania, which, on three occasions, it is alleged, furnished prohibited information in a statement regarding its activities with or in Israel, and on one occasion failed to report the receipt of a request to engage in a restrictive trade practice, will also pay $10,000.

Scope of controls

The U.S. Treasury and the Department of Commerce each have their own anti-boycott legislation, with subtle differences in scope and application. One key difference between the regimes is that while the BIS publishes details of enforcement, the Treasury does not.

There are also differences as to whom each applies. Commerce Department legislation (section 8 of the Export Administration Act, the International Emergency Economic Powers Act, and the Restrictive Trade Practices and Boycotts part of the EAR) apply to: 'U.S. persons, including individuals who are U.S. residents and nationals, business and "controlled in fact" foreign subsidiaries, with respect to activities in the interstate or foreign commerce of the United States.'

By contrast, Treasury powers under the Ribicoff Amendment to the Tax Reform Act 1976 apply to 'Any U.S. tax payer or member of a controlled group which includes such tax payer', and also includes U.S. shareholders of foreign companies.

Caveat SME

Dj Wolff, an associate at the Washington D.C. office of Crowell & Moring, has been following BIS anti-boycott law enforcement. He told *WorldECR* that while larger companies fielding sophisticated compliance teams are on top of U.S. laws, dangers lurk for those smaller companies who may not 'know anything about the Arab League, the boycott, or the boycotting laws and run the risk of violating the sanctions without having any intention to ostracize Israel.'

Activities that are prohibited by the EAR and penalized by BIS include:

- Agreements to refuse or actual refusal to do business with or in Israel or with blacklisted companies.
- Agreements to discriminate or actual discrimination against other persons based on race, religion, sex, national origin or nationality.
- Agreements to furnish or actual furnishing of information about business relationships with or in Israel or with blacklisted companies.
- Agreements to furnish or actual furnishing of information about the race, religion, sex, or national origin of another person.

Wolff says that of around ten settlements announced each year, enforcement only represents a fraction of the possible number of violations given that boycott provisions are found in many contracts drafted by Arab League and other countries, which, he warns, are not always obviously worded. 'A contract may request that the other party conforms to, for example, all UAE laws. This could be interpreted as meaning conforming to boycotting legislation. Companies recognizing a clause – or something that could be interpreted as a clause – in a contract should ask either for it to be removed, or clarified. For example, to specify that "conformity" with UAE or Saudi or Yemeni law, means "conformity with health and safety, environmental or employment law," and not with an anti-Israeli boycott.'

Higher penalties

Wolff also points out that while average settlement amounts have not typically been high (around $3,000-$4,000 per violation), that is not to say that there is not potential for more significant penalties to be imposed. There is speculation that the lower penalties reflect BIS's litigation risk assessment – sums it believes it can settle for without pushing alleged violators to the courtroom. In fact, anti-boycott regulations are currently governed by the International Emergency Economic Powers Act ('IEEPA'), which provides for penalties of up to the greater of $250,000 per violation 'or twice the value of the transaction for administrative violations of Anti-boycott Regulations, and up to $1 million and 20 years' imprisonment per violation for criminal anti-boycott violations,' according to the BIS website.

For a comparison of the two regimes, see:
http://www.bis.doc.gov/complianceandenforcement/comparison-antiboycott-laws.pdf

IATA cuts Iran Air access to settlement systems

In October, subsequent to the September designation of Iran Air as a sanctioned entity by the State Department, IATA, the International Air Transport Association, decided to deny the airline access to its settlement system and clearing house by which international ticket sales are processed and funds distributed to appropriate parties. However, the Association has registered with the U.S. State Department its belief that the designation is not appropriate.

Washington D.C.-based IATA spokesman, Perry Flint told *WorldECR*: 'After a careful and considered review, we saw that there was a possibility that the United States government would determine that we might be in violation of its laws for providing services to Iran Air. We have offices and employees in the United States and that would of course have very serious consequences for us. The law is the law; we had no choice but to suspend the airline.' However, Flint added, 'That said, we have serious concerns with a law that designates a civil aviation company. This, we feel strongly, contravenes the spirit of the Chicago Convention [the Convention on International Civil Aviation].'

According to Iran's Fars News Agency, Iran Air's managing director Farhad Parvaresh told reporters on 1 November that the company has 'managed to bypass the sanctions imposed by the International Air Transport Association', by changing its method of selling tickets – although he did not say how.

The agency said that Parvaresh had criticized IATA's decision, arguing that 'IATA is a non-governmental union which has been founded on the members' money and it is not [necessary] to comply with the U.S. sanctions laws against Iran. What was done by IATA... was the result of the U.S. administration's pressures and this decision is in essence not related to the specified duties of the union.'

EU updates

Guinea measures extension

On 27 October, the European Commission announced the extension for one year of existing measures against the Republic of Guinea.

See: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:281:0028:0028:EN:PDF

Congo changes

On 20 October, the European Commission updated the list of persons and entities in DR Congo designated by UNSCR Resolution 1533 (2004), as implemented by the Council's Decision 2010/788/CFSP.

The updated list can be found at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:276:0050:0061:EN:PDF

OFAC round-up

Iran and Sudan licensing application details published

OFAC released its quarterly report of licensing activities under the Trade Sanctions Reform Act ('TSRA') on 20 October. The report covers the processing of licence applications requesting authorization to export agricultural commodities, medicine and medical devices to Iran and Sudan under the TSRA.

The report revealed that from January to March 2011, OFAC:

- Received 428 applications for Iran licences and 44 for Sudan
- Issued 313 Iran licences and 36 for Sudan
- Issued 45 amended Iran licences and 8 for Sudan.

No applications were refused. It also revealed that the average time processing licences was 93 days, and that for 'return without action' letters it was 19 days.

New designations under Iran sanction legislation

The OFAC has designated six shipping companies which it describes as fronts for the Islamic Republic of Iran Shipping Line ('IRISL'). These companies are:

- Galliot Maritime Inc
- Indus Maritime Inc
- Kaveri Maritime Inc
- Melodious Maritime Inc
- Mount Everest Maritime Inc
- Rishi Maritime Inc.

Full details are available at: http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20111027.aspx

New licences permit food exports to Sudan and Iran

OFAC has adopted as final a previously interim rule which amends the Sudanese Sanctions Regulations and the Iran Sanctions Regulations by issuing general licences that authorize the export and re-export of 'food' to 'individuals and entities in an area of Sudan other than the Specified Area of Sudan and in Iran'.

OFAC defines 'food' as 'items that are intended to be consumed by and provide nutrition to humans or animals in Sudan or Iran – including vitamins and minerals, food additives and supplements, and bottled drinking water – and seeds that germinate into items that are intended to be consumed by and provide nutrition to humans or animals in Sudan or Iran.'

However, a small number of foodstuffs will still require specific licences for export or re-export to 'the governments of Sudan or Iran, any individual any individual or entity in an area of Sudan other than the Specified Areas of Sudan or in Iran, and persons in third countries purchasing specifically for re-sale to any of the foregoing, as well as the exportation or re-exportation of food to military or law enforcement purchasers or importers.'

Specific licences are still required also 'for the export or re-export of agricultural commodities that do not fall within the definition of food in the general licenses, medicine, and medical devices.'

Full details are available at: http://www.treasury.gov/resource-center/sanctions/Programs/Documents/gl_food_exports.pdf

U.S. professor loses tech transfer appeal

On 3 October, the United States Supreme Court denied John Reese Roth, a retired university professor, an appeal for a 2009 conviction under which he was sentenced to four years' imprisonment for breaches of the U.S. Arms Export Control Act ('AECA').

Oleg Yarko

Reese Roth worked on developing plasma actuators for drones, technologies controlled under the Arms Export Control Act.

Roth's crime was to share with non-U.S. (Iranian and, in particular, Chinese) graduate students, the fruits of his research into an ITAR-controlled project. The professor had worked with a company called Atmospheric Glow Technologies on the development of plasma actuators in development for use in U.S. Air Force drones. These technologies are controlled under AECA, which regulates the import and export of defence articles listed on the United States Munitions List, codified in Section 121 of the International Traffic in Arms Regulations ('ITAR'). Under ITAR, such technologies are controlled as technical data, and providing instructions on their use is controlled as a defence service. Transfers of ITAR-controlled items, technical data or services to foreign nationals or countries are generally prohibited without a licence. This extends to the sharing of such data with foreign nationals in the United States.

Similar cases to follow?

Sheppard Mullin partner Thad McBride advises a number of educational institutions and other research centres on their export control compliance programmes and has been following the Roth case closely. He argues that while the particulars of Roth's conviction make it unique, it still raises some questions which will only be settled by further prosecutions: 'This case is something of an outlier, in that Roth, who, it seems, was warned on numerous occasions, assured the university that he was aware of his export compliance obligations and apparently proceeded to breach them anyway. His behaviour appears to have been pretty egregious.'

And yet, says McBride, the Supreme Court's denial of Roth's appeal will place renewed attention on the case, and the more general issue of export controls in education. 'Export controls are not designed to stultify the development process,' he says. 'But there are prohibitions on sharing certain technologies with non-U.S nationals, including students otherwise authorized to be in the United States. It's got to be said that the line in the law isn't always abundantly clear; but if things have got to the point that the university is having to talk to faculty members about their teaching activities it looks as though that line is being reached.'

Much teaching is covered by what is called the Fundamental Research Exception (see box below), which

The Fundamental Research Exemption

National Security Decision Directive ('NSDD') 189, issued in 1985, states that fundamental research is not subject to the licence requirements of export control regulations.

'Fundamental research' is defined as 'basic or applied research in science and/or engineering at an accredited institution of higher learning in the United States where the resulting information, in some cases, is ordinarily published and shared broadly in the scientific community and, in other cases, where the resulting information has been or is about to be published.

Fundamental research is distinguished from research that results in information that is restricted for proprietary reasons or pursuant to specific U.S. government access and dissemination controls. University research will not be deemed to qualify as fundamental research if

(1) the university or research institution accepts any restrictions on the publication of the information resulting from the research, other than limited prepublication reviews by research sponsors to prevent inadvertent divulging of proprietary information provided to the researcher by the sponsor or to insure that publication will not compromise patent rights of the sponsor; or

(2) the research is federally funded and specific access or dissemination controls regarding the resulting information have been accepted by the university or the researcher.'

As explanatory notes on the website of Tennessee Technology University point out:

'The EAR and the ITAR approach the issue of publication differently. For the EAR, the requirement is that the information has been, is about to be, or is ordinarily published. The ITAR requirement is that the information has been published. Information becomes "published" or considered as "ordinarily published" when it is generally accessible to the interested public through a variety of ways-publication in periodicals, books, print, electronic or any other media available for general distribution to any member of the public or to those that would be interested in the material in a scientific or engineering discipline.

Published or ordinarily published material also includes the following: readily available at libraries open to the public; issued patents; and releases at an open conference, meeting, seminar, trade show, or other open gathering. A conference is considered "open" if all technically qualified members of the public are eligible to attend and attendees are permitted to take notes or otherwise make a personal record (but not necessarily a recording) of the proceedings and presentations. In all cases, access to the information must be free or for a fee that does not exceed the cost to produce and distribute the material or hold the conference (including a reasonable profit).'

allows for a great deal of technology sharing within a university setting so long as certain conditions are met. Nonetheless, McBride says, export controls can create real tensions between faculty staff and university management: there is an inherent conflict between an academic institution's role as a facilitator of knowledge and the restrictions placed by export controls, even when those controls are intended to further the purpose of national security.

McBride believes that the challenge for universities and other research centres is having the right infrastructure in place to ensure that staff are aware of the applicable laws – and that the government is actively enforcing them: 'The more sophisticated research institutions in the game for a while either have experienced outside counsel or some compliance team who actively review contracts, and grants, corporate work etc.'

Controls focus on nationality

A key feature of the ITAR regime of course, is that it applies to virtually every country in the world, and thus, in theory, the scope of enforcement is extremely broad. But McBride suggests that a prosecution would have been much less likely had the plasma technology been shared with, say, an EU or Australian national: Iranian and Chinese nationals are far more likely to be on the figurative radar screen, raising the question of selective enforcement. For example, in the case of naturalized citizens or lawful permanent residents of the United States of Iranian or Chinese origin, 'the U.S. government very well might say that if technology is shared [with such persons], then, given U.S. concerns, there could be a heightened duty to look at their connections, for example family ties, or how often they visit the countries in which they were born.'

When may the institution itself be liable?

The Roth conviction was a headline case and from the facts, it is evident that the University of Tennessee did everything that it could to make the professor aware of his potential violations, and to warn him from continuing. But an interesting question (which the particulars do not answer) relates to the liability of a university or research facility in the event that they were found to have failed to have taken the necessary steps – either through sufficient awareness training or disciplinary action – to have prevented the transfer from having taken place. 'Had that been the case,' says McBride, 'it would have been interesting to see whether the government would have focused on the university instead of the individual professor.'

Clearly, this is a difficult area for all concerned. It has a bearing on the respective roles of universities as flag bearers of knowledge, but also custodians of national security – and also begs questions as to the limits of what can legitimately be published in academic research journals or on the internet. 'Once something is out there in the public domain, it's very difficult to claw back,' McBride points out.

Because they deal with the transfer of intangibles, deemed exports are very much more difficult to prove/police than the exports of hardware; but the potential damage that breaches can cause is no less real. Which is why, says McBride, the U.S. government is hungry to make examples where it can. 'It's a hell of a wake-up call for universities and their faculty,' he says. And a particularly unpleasant one for John Reese Roth.

Putting its money where its mouth is

Many talk about their commitment to export controls compliance but rare is the company that embarks on a global audit of its systems and voluntarily discloses the findings to the authorities. Scott Sullivan speaks to *WorldECR* about Flowserve's recent $3m settlement with OFAC and BIS.

On 3 October Flowserve, a U.S.-headquartered provider of flow control products and services, announced it had entered into settlement agreements with both the Commerce Department's Bureau of Industry and Security ('BIS') and the Treasury Department's Office of Foreign Assets Control ('OFAC') for voluntary disclosures of breaches of export controls and economic sanctions under which it is to pay a combined penalty of around $3 million. The company's multi-site internal review which culminated in the settlement is perhaps the largest ever undertaken, covering over 40 sites around the globe, and as such represents a landmark investigation. It was both a painstaking and sometimes intense process, as *WorldECR* discovered when it spoke to Scott Sullivan, Vice-president, Global Trade, Compliance & Corporate Inquiries, and a core member of the investigation team.

Sullivan: 'We were determined to right the ship and restore our reputation with the authorities.'

Catalyst for change

It was an Export Administration Regulations ('EAR') rule change that first alerted Flowserve to the possibility that not all was as it should be on the export control front. In April 2005, BIS amended the EAR to strengthen export controls on equipment and technology designated as having potential use in chemical or biological weapons programmes. The result was to increase the number of countries requiring a U.S. export licence in order to export or re-export controlled products sold by pump/valve manufacturers from around 37 to over 150 – with potentially drastic repercussions both for the company's business and its compliance record.

In the spring of 2006, Sullivan was due to undertake a general review of the company's control processes when he discovered a number of potential violations: 'So we sat down with management and walked them through some of the issues,' he recalls. 'Given what we found at a few sites, we realized that there could be other things out there. That was March 2006 and that's when we started looking at a more comprehensive review programme to determine our compliance, or lack thereof, with export controls.'

A key issue for the company was that like many others, Flowserve is essentially 'a conglomeration of conglomerates'. Everything, says Sullivan, was decentralized 'and everyone was doing everything their own way. There wasn't great communication internally over rule changes, so some people were doing things under old rules while there was a general lack of understanding regarding the new rules.'

A common finding was general misunderstanding of U.S. rules and regulations on the part of non-U.S. persons, some of whom 'had misunderstood the meaning of some very complex regulations and over the years were acting under the belief that X was ok and Y was not when those weren't fully accurate interpretations.' This was complicated by a reluctance among some to raise issues they thought they were prohibited from raising with U.S. persons: 'Typically, what happened was that non-U.S. persons, when they heard the words "Iran", "Sudan" or "Syria", didn't want to talk to their U.S. colleagues because they were afraid that they'd get them into trouble. So, it became a self-reinforcing problem. They didn't want to taint the transaction and get their colleagues in trouble. That was the scenario – a perfect storm.'

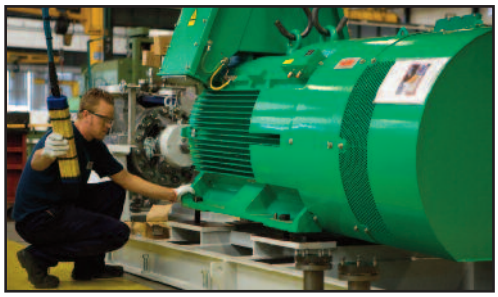
Rolling out the review

The review process was a major operation, commencing with classification of hundreds of the company's sites. 'Of each one we asked: Is it a manufacturing facility? Is it a service centre? Is it domestic sales only? Is it export? And so on. Then we issued survey questionnaires and gathered a vast amount of data which we went through to determine which sites we needed to visit and what might be the risks for each. This was a lot of work, involving multiple ERP systems, multiple languages, and generally a whole host of jurisdictions and legal systems to

Flowserve's export compliance statement

Flowserve Corporation, recognized as one of the world's premier providers of flow management systems, has a firm commitment to product integrity, security and compliance with US and/or local export laws and regulations. Under no circumstance will Flowserve knowingly export products and/or technology contrary to US and/or local export and import laws and regulations.

The company's compliance commitment is underlined by its trade compliance policies on its website. See: http://www.flowserve.com/About-Flowserve/Corporate-Information/Trade-Compliance



deal with.'

Flowserve involved outside counsel (U.S. law firm Kelley, Drye & Warren, with partner Eric McClafferty as lead lawyer), from 'the get-go'. Sullivan's view is that bringing in help early on 'provided greater independence, additional expertise, and constructive engagement with government regulators,' than would have been possible had the company engaged a firm further down the road, though he is keen to point out that it was important that the company did not use the external counsel as a bulwark between itself and the government agencies. 'It wasn't as though we handed it off directly to outside counsel,' he says. 'I think generally it was more like a symbiotic relationship which leveraged the strength of each of the parties. We know the business and the operations. Outside counsel is an expert on the law. So we were able to pair those two up and develop a lot of quick processes and evaluative tools in identifying where we had problems and risks.'

It was a process that wasn't without a degree of pain and discomfort. 'We opened the kimono completely. We're the only company on the books presently that has done a true, full global disclosure. Most companies have done one or two sites or maybe three. But we essentially went to all our significant manufacturing sites and beyond, and did a full five-year look back. We looked at literally millions of transactions – and the breaches that we did disclose do have to be seen in that context.'

A whole lot of obstacles

The challenges were myriad, especially given the international nature of the investigation: 'You've got to consider the issue of attorney/client privilege. And you've got to consider data privacy, which is particularly an issue in Europe. If you're doing email searches for example, it's important that you're careful that they're done according to all the applicable rules and even policies in certain jurisdictions. This can be very time consuming.'

And on a practical note, there were naturally issues to do with language: 'When you're conducting interviews that potentially involve legal liability, you've got understand what you're asking.'

This was not a cheap process, and while Flowserve hasn't put a price tag on it Sullivan suspects that the cost easily matched the settlement figure. The bulk of the money was spent on law firm fees: 'Most of the translation was done internally. But it cost a great deal in management and employee time, IT resources to pull data – though the law firm we used did have a data mining group which was very cost-effective; it meant that we could use the consulting arm of the firm to assist in analysis and so reserve the higher paid lawyers for the major issues. We worked pretty hard to do it right but also in the most efficient, cost-effective manner.'

Sullivan believes the road to efficiency lay in being methodical: 'We had an export compliance team in place. We beefed up that team, and then also brought in project managers, and then physically mapped and planned out the entire disclosure process: time on site, topics to be covered. At each site, we did transactional audits, policy and procedural review and enhancement and we also undertook training.'

Typically the team would include one or more often two lawyers from Kelley, Drye & Warren, two people from the internal export control compliance team and one project manager. 'At each site we have an export compliance coordinator. We were at a site for anything between one and two weeks reviewing the data, doing interviews, doing training, analyzing policy and procedure, reviewing transactions and all those kinds of things – quite a few hours on planes and time away from home.'

Cultural awareness

Aside from the logistic and people management issues in such an exercise, Sullivan points out there are intrinsically human and political considerations that need to be borne in mind. 'One of the things that we found – and there's a great deal of sensitivity around this issue – is that it can be difficult for non-U.S. people to accept the extra-territorial jurisdiction of the United States. There's a lot of essentially political resentment and anger about America, or Americans, extending our grip overseas.'

This issue, suggests Sullivan, has to be fronted within any multinational: 'Ultimately the way that we successfully navigated this was by having internal political discussions about things such as sanctions programmes and anti-boycott rules – often informally, for example over lunch or after training sessions. I might say, "I'd love to smoke a Cuban cigar sailing down the Nile into Sudan while eating caviar on a Persian carpet but I can't." That's the corporate reality of being a U.S.-headquartered, publicly traded company. It might not always be fair but it is what it is and it should be treated as a business requirement.'

Flowserve at a glance

- Founded: In 1997 with the merger of BW/IP and Durco International
- Core Business: Manufacture engineered and industrial pumps, industrial valves, control valves, nuclear valves, valve actuators and controls and precision mechanical seals and related sealing support systems, and provide a range of related flow management services, primarily for the process industry
- 15,000+ employees in 50 countries
- Customers in more than 70 countries
- Sales: $3.24bn, up 12.2% on previous year

That settlement in full

The total $3million package to be paid by Flowserve represents two settlements conjoined, one with BIS and one with OFAC. 'Both the agencies have their own internal calculation methods. BIS has a "FOIA" room [Freedom of Information Act reading room], so what we did was look back to try to find analogous or similar cases. Because we did a voluntary disclosure, that typically represents a 50% cent mitigation, and BIS also further mitigated our penalty by taking into consideration other remedial factors like enhanced policies and proecedures. We ended up proposing a settlement amount and while there's a little bit of back and forth, at the end of the day we came out with a fair settlement. We were keen to wrap the whole thing up, put it behind us, and continue to move forward as a company.'

The way forward

Sullivan says he hopes to never again be in the position of having to do another global disclosure – but recommends

similar organizations consider the process: 'Given the complexity of the regulations, companies may be fooling themselves into thinking that they don't have issues or problems around. Having a compliance programme in place can minimize, or mitigate but it can't eliminate. Human error is recognized by the Commerce Department as one of the top five reasons for export violations occurring. However much you systematize and put in IT programmes, you're going to be in the position at some point of having to make disclosures.'

'However much you systematize and put in IT programmes, you're going to be in the position at some point of having to make disclosures.'

In the future, thinks Sullivan, there's going to be a greater expectation on the part of the authorities that companies with a major multi-jurisdictional presence will conduct increasingly thorough internal investigations of the kind that Flowserve undertook.

'You're almost left to answer a negative,' he says. 'If you have major multinational presence, you're likely to have t consider whether you have systemic problems. If you go to site A and you identify some problems and you say, "Here's our disclosure, thank you very much," increasingly the response to that is going to be, "Well, how do you know that you don't have similar problems at site B or C, D?' It all depends on the jurisdictions that you're in, on the nature of the items that you've uncovered. Just as there are now global investigations in the FCPA arena, the same is starting to apply to export controls and if you uncover one problem, you're effectively left to prove that the same problem isn't occurring elsewhere.'

Sullivan believes that electronic filing has enhanced the ability of regulators to detect issues, adding, 'And now after 9/11 there's a lot more information sharing within the U.S. government but also between other governments.' This, he argues, is bound to result in a greater number of global, multi-jurisdictional prosecutions in the future.

And the benefits?

An undertaking on such a scale is a thorny nettle, touching not only on compliance and processes but also underlying issues including company identity and cohesion, internal communication and different attitudes to risk. So why grasp it?

Sullivan is clear that Flowserve did the right thing: 'I think it was just something about the culture of the company that we wanted to do so. We were determined to right the ship, clean the slate, and restore our reputation with the government authorities. We worked hard to do that. And in so doing we've bettered the company and we're much stronger.'

Feature: Asia export controls

Cross-winds blowing in the East

Does the arrest of four Singaporean citizens following a request by the U.S. that they be extradited to face charges of illegally exporting US-made radio equipment to Iran signify a tightening of export control laws is Asia? Tom Blass reviews the evidence.

On 26 October, it was announced that the government of Singapore had arrested four Singaporean citizens following a request from the United States that the four be extradited to face charges for exporting radio equipment to Iran which was subsequently used in roadside bombs in Iraq. Wong Yuh Lan, Lim Yong Nam, Lim Kow Seng and Benson Hia Soo Gan were accused of breaching international sanctions following a U.S. Justice Department investigation that uncovered a conspiracy to ship 6,000 radio frequency modules from a Minnesota-based company in the U.S. through Singapore to Iran. According to reports, the modules, which could transmit wirelessly for up to 40 miles, were ordered for a Singapore telecommunication project but were then re-directed to Iran.

The response to the extradition request would appear to evidence the United States' continued extension of its extra-territorial jurisdiction to the East. But does it also signify an increased willingness on the part of the Singaporean authorities to embrace international sanctions and export controls? And if it does, should observers expect to see other Asian countries seriously stepping up their anti-proliferation efforts?

Export controls in Asia

Export control policy and practice in Asia is a patchwork of economic, political and geopolitical drivers and its realities are often obscured: 'It isn't always possible to know what's actually going on or why,' one export control lawyer said. 'Generally you only get to find out what governments want you to know.'

The response to the extradition request would appear to evidence the United States' continued extension of its extra-territorial jurisdiction to the East.

Export control regimes across Asia have on occasion come under fire from the West for being ineffective or even invisible. For example, following the exposure of the AQ Khan network in 2004 (see the box 'Malaysia, AQ Khan and the Strategic Trade Act'), Malaysia came under sustained pressure from the United States to improve its policing and controls of anti-proliferation activities. The result was the introduction last year of new legislation and new enforcement powers (see 'Malaysia's new Strategic Trade Act', *WorldECR* issue 1). Such pressure is unlikely to ease and today it extends across the region. How the different Asian countries respond to it remains to be seen.

Wendy Wysong, partner at the Hong Kong office of Clifford Chance, says that there's an 'ebb and flow' to the dynamic of export controls and anti-proliferation efforts (not only in Asia but elsewhere) as countries weigh the relative national security advantages of exerting stronger or weaker laws: 'While it may seem that restrictive laws are most effective in protecting national security, in some cases such restrictions actually undermine national security. Restrictions that are too strong encourage companies to move their operations and expertise elsewhere, thereby costing the overly restrictive country any degree of control at all over that technology as well as the technological edge that company provided. Moreover, stronger controls can slow down the process of getting technology to allies, encouraging buyers to look for alternative sources. Companies in less restrictive countries are incentivized to reverse-engineer products or even resort to theft of industrial secrets in order to meet the demand.

'On the other hand, Asian countries are also realising that if they have a well-developed system they can say to, for example, the U.S. and its allies, "Look, you can trust us with exports because we have sufficient safeguards

Feature: Asia export controls

in place that you can lower yours with regard to us." We're seeing that line of argument in Hong Kong and Singapore, and attempts to adopt similar positions by India and China, for example.'

Edmund Sim, a partner at the Singapore office of Appleton Luff, also sees the pull and push of factors affecting the way that export controls function in Asia. And while some commonalities are shared between countries, the dynamics of each are often unique, if not dissimilar. According to Sim, 'Singapore, for example, as one of the world's most important transhipment hubs, is very anxious to be seen to be supportive of U.S. anti-proliferation efforts. That's largely the same for Hong Kong. But for low-cost labour economies such as Vietnam, for example, and to an extent Thailand, the incentive for strengthening their regimes lies in their need to attract Japanese investment in order to thrive.'

Japan is the largest foreign investor into Thailand, typically accounting for around 40% of inward investment: according to the Thai Board of Investment, in the first five months of the year, Japanese investors applied for investment incentives for 221 projects valued at Bt57.438 billion. That was from a total value of all investment applications during the period of Bt141.196 billion.

Vietnam, likewise, courts Japanese investment: on 2 November, following a meeting with 20 Japanese business heads, Prime Minister Nguyen Tan Dung publicly welcomed public-private partnerships with Japanese business to develop his country's infrastructure.

Such appetite for Japanese investment may prove to be the United States' greatest aid in fighting proliferators. Investment on this scale could influence the development of export controls and enforcement in the region. As Edmund Sim continues: 'Japan has made it very clear that it is not going to invest in high-end industries unless those countries have sufficient export controls in place – and for this reason: Japan is very dependent on U.S. investment and companies; it is a major supplier, for instance, to Boeing's 787 programme. This means that they have to take proliferation measures very seriously. In turn, they're pushing other regional economies in order that they can outsource assembly operations outside of Japan, where production is cheaper. Gradually, those countries are waking up to the realization that they will lose out unless they, too, take the issue seriously.'

Different views

Of course the picture changes from country to country. Observers on the ground comment that not all jurisdictions are equally equipped to introduce new legislation: 'This [improving export controls] isn't high on the agenda in Indonesia or the Philippines, which don't actually have the capacity to enforce their existing import/export laws,' says one.

Indeed, there remain concerns that

Malaysia, AQ Khan and the Strategic Trade Act

In April 2010, Malaysia enacted a new law to address loopholes which had left it vulnerable to being exploited by those involved in nuclear proliferation. This was in response to mostly U.S. pressure and also in recognition that Malaysia had been perceived as being lax in its efforts to block weapons of mass destruction ('WMD') proliferation.

It was the use of Malaysia as a transhipment hub by the Pakistani nuclear scientist AQ Khan that most aroused U.S. concerns. In 2004, Khan confessed that he had orchestrated the transfer of WMD technology to a number of countries, including Iran, North Korea and Libya, largely with the assistance of a Malaysian-based middle-man, Buhary Syed Abu Tahir, who procured from a Malaysian company, SCOPE, several thousand high-precision aluminium centrifuge parts for use in the manufacture of nuclear weapons. The parts were later intercepted aboard a ship BBC China, bound for Libya.

At the time, Malaysia was a signatory to the Nuclear Non-proliferation Treaty ('NPT') but did not participate in the Zangger Committee or the Nuclear Suppliers Group ('NSG'). Nor were the components controlled by any national legislation – thus SCOPE was not actually in breach of the law, according to domestic interpretations of both Malaysian law and the terms of the NPT at the time of the BBC China's interception.

Subsequent cases with a Malaysian dimension further heightened fears about the efficacy of the country's legislation. In the past three years, the United States has charged, convicted or sentenced defendants in at least six cases involving transfer of U.S. military technology through Malaysia (according to the anti-proliferation group NTI).

The 2010 Strategic Trade Act outlaws the shipment of weapons of WMD and related materials through Malaysian territory. It defines WMD as '[A]ny weapon designed to kill, harm or infect people, animals or plants through the effect of nuclear explosion or dispersion or the toxic properties of a chemical weapon or the infectious or toxic properties of a biological weapon, and includes a delivery system designed, adapted or intended for the deployment of such weapons.'

The law authorizes the appointment of a Strategic Trade Controller to establish and coordinate a unified licensing system for trade in strategic materials, and further extends the control over strategic items being trans-shipped through Malaysian ports.

However, some observers have argued that while the move is positive, it is at odds with the country's economic objectives; with academics Stephanie Lieggi and Richard Sabatini from the Monterey Institute for International Studies having stated in a 2010 paper that while commendable as a first step 'ensuring that Kuala Lumpur prevents future trans-shipments or exports of sensitive dual-use goods will remain difficult. Given the critical importance of exports of high-tech goods to Malaysia's economy, many within the domestic system will remain reluctant to block shipments without clear proof that the goods in question are destined for a weapons purpose—a very difficult standard to meet.'

They also argue that this 'reluctance' is characteristic in South East Asia, and manifest in a generally 'lukewarm' appetite for implementing UN Security Council Resolution (UNSCR) 1540 which 'mandates that states establish and enforce effective measures against the proliferation of weapons of mass destruction, their means of delivery and related materials, thereby attempting to stem WMD proliferation to state or non-state actors'.

Feature: Asia export controls

some Asian governments have yet to fully take on board the underlying reasons behind international export control regimes, which may explain why some appear to take their implementation less than seriously.

Sim points out that while the Association of South East Asian Nations ('ASEAN') has a Treaty on the Southeast Asia Nuclear Weapon-Free Zone and Declaration for a Zone of Peace, Freedom and Neutrality (Zopfan), there is a feeling in some parts that export controls are 'driven by the West, particularly the United States', and that they go too far, in effect discouraging the export of items which present no security threat.

In one marked respect, ASEAN countries have a very particular take on their region, with some quarters making a collective call for a relaxation of sanctions against Burma/Myanmar, something that is at odds with the West's policy. This, of course, is not a proliferation issue, but it does serve to highlight the extent to which there are real differences between the United States and Europe and even countries which they regard as close allies.

One lawyer at the Hong Kong office of an international law firm points out that until April this year Hong Kong had not implemented UNSCR 1929 against Iran (which was passed in June of last year). It did so, notably in response to EU and U.S. pressure, who sought the closure of some significant loopholes with respect to U.S. blacklisted HK shipping companies. It is unclear how strictly the implementing law is actually being enforced. 'It is my impression,' says the lawyer, 'that companies in the region are continuing to do business with sanctioned companies for the reasons that it is an established part of their business activities, that other companies do it, because of lack of knowledge of the rules and perhaps because of a lack of enforcement.' This lawyer adds that, in their experience, there is a noticeable lack of awareness of the various sanctions regimes amongst companies in the region, despite the fact that many 'employ or are run by EU and U.S. nationals'.

It is of course arguable that given the fact that many of the region's governments are neither members nor signatories to certain export control regimes and treaties, that is simply to be expected (see table, above). What business leaders in those countries may be failing to understand, however, is that that is not a defence for turning a blind eye to proliferation activities in the mind of the United States.

Member and signatory? Yes or No?	China	Indonesia	Malaysia	Philippines	Singapore	Thailand	Vietnam
Australia Group	N	N	N	N	N	N	N
Biological Weapons Convention	Y	Y	Y	Y	Y	Y	Y
Chemical Weapons Convention	Y	Y	Y	Y	Y	Y	Y
Comprehensive Test Ban Treaty	Y	N	Y	N	Y	Y	Y
Missile Technology Control Regime	N	N	N	N	N	N	N
Nuclear non-proliferation treaty	Y	Y	Y	Y	Y	Y	Y
Nuclear Suppliers Group	Y	N	N	N	N	N	N
Proliferation Security Initiative	N	N	N	Y	Y	N	N
Wassenaar Arrangement	N	N	N	N	N	N	N
Zangger Committee	Y	N	N	N	N	N	N

Source: BAFA. This table does not purport to be exhaustive.

Other lawyers in the region report that while they often run training sessions and briefings for local business, certain companies are looking closely at the parameters of the law as much to understand what doesn't apply to them as what does and so be able to profit. Clifford Chance's Wendy Wysong explains: 'We give training on CISADA all over Asia, and ensure that our clients know what they need to in order to remain compliant. We're asked to review transactions and sometimes it's clear that a party is trying to take advantage of opportunities that arise by virtue of the fact that they're not directly covered by U.S. or EU sanctions regulations. Then we can't get involved.'

This is a not uncommon observation. Other lawyers at EU- and U.S.-headquartered firms say that they back out of any discussions when it becomes apparent that their clients are looking at taking advantage of sanctions regulations that don't apply to Asian companies.

Will to enforce

Despite these concerns, it seems that certain Asian companies – arguably those with an eye to their future international reputations – are anxious to be seen to be abiding as much by the spirit of anti-proliferation regimes as by the letter. And that, according to Edmund Sim, is arguably, in microcosm, the approach of the countries themselves. 'Singapore is certainly more public [than some others] about enforcement, but it isn't transparent,' he says. 'That's very much the Asian way. Just as with the case of the extradition of arms dealer Viktor Bout, you won't find out about some of these things unless the government has reason for wanting it in the public domain. It's very much along the same lines as enforcement of the Foreign Corrupt Practices Act. For a long time, you just couldn't say how many people, were being extradited for breaching it.'

The point is echoed by Wendy Wysong, who says that just because there's little information about enforcement available, that's not to say that it doesn't happen: 'Enforcement does happen – I'm currently working on investigations in Hong Kong and Taiwan – and I'd say that every company has an interest in making sure that it doesn't give any enforcement agency anywhere an excuse to make things difficult for them.' But the details remain effectively shrouded, except to insiders who rely on word of mouth and industry information-sharing as a

Feature: Asia export controls

China's export control regime

Relevant laws and regulations

China based its export control regulations on the Foreign Trade Law, which was amended in 2004 and took effect on 1 July 2004. China has separate export control regulations on chemicals, biological agents, missiles, nuclear goods and related technologies, and catalogues of products subject to export control. The Ministry of Commerce ('MOFCOM') issued the regulations on import/export licensing of dual-use items and technologies and updates the catalogue of dual-use items and technologies subject to import/export licensing on a yearly basis from 2007.

Main competent government agencies

1. State Council (China's cabinet): It sets overall export control policy, but does not get involved in day-to-day licensing matters. However, licensing issues are discussed within the State Council when issues of state security are involved or when there is disagreement within the system. The State Council has the authority to invoke catch-all provisions and can add items to the existing control lists.

2. Central Military Commission ('CMC'): Senior officials from the CMC meet with State Council officials to discuss export policies, mainly those related to military exports; 'major' military exports and contracts must be examined and approved by the CMC and the State Council. Note, however, the CMC does not play a role in vetting exports of nuclear or chemical materials, equipment or technologies.

3. Ministry of Commerce ('MOFCOM'): The Department of Mechanics, Electronic and High-Tech Industry ('DMEHT') within MOFCOM has the primary authority on

(i) formulating and implementing national policies on import/export control and rules on import/export of dual-use goods and technologies;

(ii) approving import/export licences for dual-use goods and technologies as well as precursor chemicals;

(iii) coordinating the enforcement of laws and regulations on import/export controls across regions and governmental agencies;

(iv) undertaking the work of expert committee on export control on dual-use nuclear goods and related technologies;

(v) issuing end-user certificates for dual-use goods and technology import; and

(vi) supervising and managing end-users.

Other ministries, such as Agriculture, Health, and Science and Technology also play a consultative role and are called upon by MOFCOM to advise on individual licences.

4. State Administration for Science, Technology and Industry for National Defense ('SASTIND'): Under the jurisdiction of the Ministry of Industry and Information Technology ('MIIT'), SASTIND has an important role in regulating China's exports (and possibly imports) of sensitive military items, and in vetting all of China's conventional military exports, including missile-related exports. SASTIND also has influence over the vetting of nuclear exports. China Atomic Energy Agency ('CAEA') under SASTIND is responsible for vetting applications to export nuclear materials, equipment and technology. (Nuclear related dual-use items are vetted by MOFCOM in consultation with SASTIND and CAEA.)

5. General Armaments Department ('GAD'): It plays an active role in the export control review process. For example, GAD is responsible for controlling exports of nuclear materials. GAD also has a hand in vetting exports of military products and certain missile systems along with other agencies such as MOFCOM.

6. Chemical Weapons Convention Implementation Office ('CWCIO'): It reviews applications for exports of chemicals listed in the Chemical Weapons Convention ('CWC') (Other chemical items are vetted by MOFCOM). Applications for transfer of scheduled chemicals (i.e. items on the CWC schedule of chemicals) first go to the CWCIO and are then passed to MOFCOM for final licensing approval. To assist in application vetting, the CWCIO maintains a hotline with MOFCOM, GAC, and MOFA.

7. General Administration of Customs ('GAC'): It is the enforcement bureau for export control. It is responsible for inspecting exports before they leave China to ensure they have the appropriate export licenses and transit documents. Export companies often first go to the GAC before applying for a licence in order to determine if an item is subject to China's export control regulations. The GAC has a computer database listing controlled items.

8. Ministry of Foreign Affairs ('MOFA'): The Department of Arms Control within MOFA reports on issues such as international arms control and export control, and participates in China's export control legislation and policy-making.

Courtesy of White & Case LLP

© wanchai

Feature: Asia export controls

means of taking soundings as to what's occurring behind the scenes.

Chinese whispers

The situation in China is, of course, quite different to that which prevails elsewhere in the region. China regards itself (rightly) as a political and economic powerhouse and one which will only bow to outside pressures when it is clearly in its own interest to do so. There is, say lawyers on the ground, considerable dialogue at government to government level between China and the outside world, including information sharing and sharing of best practices. But export controls remain a tricky issue for companies doing business in the Middle Kingdom. As one lawyer notes: 'Look at the Rio Tinto "state secrets" case in 2009. It was a typical example of the government seizing on something for political reasons and inflating it.'

According to one Beijing-based lawyer, in more than five years of his working in China, he has not seen any high-profile or stringent application of export control legislation. That's not to say, he points out, that businesses shouldn't endeavour to keep their '…I's dotted and T's crossed…'. But on paper at least, the regime is complex, and characterized by 'a mish-mash of agencies and authorities' (see 'China's export control regime' and the article by Chris Cloutier and Jane Cohen in this issue) and various lists of categories of restricted and prohibited technologies.

The implementation of the controls that do exist is further complicated by the fact that enforcement of the law in China is not consistent across the country. As one lawyer comments: 'In general, I think that the government is trying to be fair; that is, it tries to apply the law equally to foreign and domestic companies. But there is definitely a discrepancy, and sometimes a tension, between provincial governments and central government. The former are probably more likely to exhibit favouritism, taking the attitude, "We are far from the Emperor…".'

To the future

Perhaps it could be said that it is a general uncertainty as to the location of "the Emperor" (Is he in Beijing, Bangkok, Tokyo or Washington?), that sets the tone for anti-proliferation policy, legislation and enforcement in Asia at large. The situation may be becoming clearer, but the wide range of competing factors is always likely to prevent it from being straightforward.

Tom Blass: tnb@worldecr.com

Today, the rules apply to everyone

Scott Sullivan of Flowserve offers a fascinating insight into the work of an in-house export controls practitioner in a major multinational. During an internal investigation into possible breaches of U.S. export controls in more than 100 of the company's sites around the world, Sullivan and his team uncovered obstacles to compliance that they never expected. Such a glimpse into the day-to-day activities of those on the 'front line' isn't easy to come by – the data gathering, translation, cultural challenges, and interactions with government agencies – and we're delighted to be able to present it in this issue. To the best of its ability, Flowserve left no stone unturned in its efforts to get things right. And given, as Sullivan pointed out, that the company is a 'conglomerate of conglomerates' (like so many corporations), this was not the easiest thing for the corporation to ask of itself. We applaud Flowserve's initiatives and efforts. The company can look to the future with a clean bill of health.

Of course, Flowserve is a multinational with the resources to spend – both on the investigation, and also on the settlement. And it's becoming apparent that while enforcement agencies are focusing much of their attention on high-profile, multi-million or billion dollar turnover companies, that certainly doesn't represent the full extent of their interest.

Increasingly, being large does not place a company above the law; nor does being small place it below the radar.

Smaller companies are fair game for investigation, as are individuals – like John Reese Roth, the Tennessee professor whose continued breaches of the ITAR in a university setting have earned him a four-year prison sentence, his appeal having failed. The circumstances of professor Reese Roth's case may have been very particular – but there will be a raft of academic institutions across the U.S. and Europe who will be studying those particular circumstances to make sure that they bear no resemblance to their own and that the Chinese students they are so actively targeting for future fees will not render them and their academics guilty of similar breaches.

Every issue, we aim to provide our readers with insights into the export control laws of jurisdictions which might otherwise be quite literally alien to them. On paper of course, there are often similarities and common sources. This time round, we wanted to take soundings from those on the ground – in a number of Asian countries in this instance. The resounding message was that for a number of reasons, security-related and economic, export controls are gradually being ratcheted up – although progress is patchy and laws often selectively enforced.

The latter point, say observers, means that businesses should take extra care to ensure their compliance for, increasingly, being large does not place a company above the law; nor does being small place it below the radar.

Tom Blass, November 2011
TNB@worldecr.com

CISADA and the expansion of U.S. sanctions against Iran


The Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 ('CISADA') broadens the scope of sanctions that can be imposed on those engaged in business activity with Iran. Jason M. Waite and Diego S. Marquez consider its impact.

On 1 July 2010, President Obama signed the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 ('CISADA') into law. This expansion of U.S. sanctions, and the sanctions imposed by the United Nations and the European Union in the Summer of 2010, and by Japan and South Korea in September 2010, suggested a growing global consensus on the need for the international community to further isolate the Iranian regime.

One year later, as this article goes to press, news of an alleged Iranian plot to assassinate the Saudi ambassador to the United States in a Washington restaurant has heightened concerns in the U.S. capital about the Iranian regime and CISADA has come under review in the United States Congress as the government considers further actions.

CISADA goes further than the Iran Sanctions Act in terms of its scope of prohibited activity and provides for new 'triggers' that would require the imposition of sanctions.

This article summarizes the changes enacted through CISADA to expand the scope of sanctions that may be imposed against companies engaged in certain activities, the steps that the Obama administration has taken to implement the new sanctions over the last year, and how the expanded sanctions have impacted the worldwide business community. The article then offers recommendations for companies interested in maintaining compliance to avoid the imposition of the expanded sanctions, and concludes by considering the types of additional actions that could be taken by the United States.

CISADA: expanding the scope of existing sanctions

CISADA amends the Iran Sanctions Act ('ISA') to broaden the scope of sanctions targeting investments in Iran's energy sector. In particular, CISADA expands the activities subject to sanctions and establishes additional sanctions that can be imposed on those engaged in such activities.

The ISA authorized sanctions on any person that (1) invested more than $20m in the enhancement of Iran's ability to develop petroleum resources or (2) exported, transferred or otherwise provided to Iran goods, services, technology or other items knowing that the provision of such items would contribute materially to Iran's ability to develop or acquire weapons of mass destruction or certain other advanced weapons. The new sanctions under CISADA similarly target investments ($20m or more or $5m per investment, totaling $20m or more in a 12-month period) that directly and significantly contribute to the enhancement of Iran's ability to develop its petroleum resources. However, CISADA goes further than the ISA in terms of its scope of prohibited activity and provides for new 'triggers' that would require the imposition of sanctions.

Specifically, CISADA provides that the President must impose sanctions against a person he determines 'knowingly' sells, leases or provides any of the following, when such items have a fair market value of $1m or more or an aggregate fair market value of $5m or more in a 12-month period:

- goods, services or technology that could directly and significantly facilitate the maintenance or expansion of Iran's domestic production of refined petroleum products;
- refined petroleum products (to Iran); or
- goods, services or technology that could directly and significantly contribute to the enhancement of Iran's ability to import refined petroleum products.

While the law requires persons to act 'knowingly', that term is defined to include both actual knowledge and constructive knowledge.

Congress identified the refined petroleum industry as a vulnerability of the Iranian regime; at the time of CISADA's passage into law, Congress estimated that Iran imported between 25% and 40% of its refined oil needs due to limited domestic refining capacity. Believing that refined-petroleum-related sanctions could have a significant impact on the Iranian economy, Congress targeted more than the mere sale or provision of refined petroleum products or significant investments in the Iranian oil industry. The 'triggers' for the imposition of sanctions extend to a wide range of activities that could enhance Iran's refining capacity or assist in the delivery of refined petroleum products. The triggers now include assistance in the construction,

modernization or repair of petroleum refineries, including through the sale of parts and equipment, or the transfer of technology, as well as less direct contributions to Iran's refined petroleum industry, such as certain insurance or reinsurance services, financing or brokering services, the supply of ships and the provision of shipping services.

Prior to CISADA, the President had available to him a menu of six options from which to choose sanctions once a determination was made that an entity was violating the ISA. Now, under the ISA as amended by CISADA, the President has three new options available on the menu of sanctions, options that specifically target access to financial services by allowing the President to prohibit foreign exchange transactions and banking transactions, and broad authority to block property subject to U.S. jurisdiction. The chart 'Available sanctions' lists the sanctions that may be imposed by parties found to be engaged in prohibited conduct.

The newly available sanctions are significant in their scope; the prohibition on transactions with respect to property subject to U.S. jurisdiction, for example, essentially means that an entity subject to this sanction is prevented from doing any business with U.S. persons even where that business takes place entirely outside the United States. The impact is likely to be felt by a sanctioned party even more broadly than is actually intended given the practice of many global companies to screen all of their worldwide transactions against lists of prohibited parties and their tendency to avoid business with such parties as a prophylactic matter, even if U.S. persons may not be involved in the transaction. Indeed, the three additional sanctions greatly expand the President's power to reach foreign entities doing business with Iran.

There are additional provisions of CISADA beyond those described above. These include provisions calling for the imposition of sanctions on foreign banks that knowingly facilitate Iranian efforts to acquire weapons of mass destruction or engage in doing business with key Iranian banks, the Iranian Revolutionary Guard Corps ('IRGC') or entities sanctioned by the UN Security Council. U.S. regulators have been active in implementing these requirements, including in a rule promulgated by the Treasury Department's Financial Crimes Enforcement Network ('FinCEN;), effective 11 October 2011, that requires U.S. banks, upon request from FinCEN, to inquire of certain foreign banks for which the U.S. bank maintains a corresponding account as to the activities of those banks with respect to certain parties of concern. Administration officials have indicated that FinCEN has already issued requests to certain foreign banks suspected of dealings with designated entities.

CISADA also includes provisions targeting officials responsible for human rights abuses, exporters of technology used to restrict communications, and countries that allow for diversion of certain goods, technologies and services. It imposes new requirements on U.S. government contractors and grants state and local governments the authority to adopt and enforce measures to divest government funds from entities engaging in business with Iran's energy sector. Indeed, many state pension funds have begun reviewing the activities of companies in which they are invested and divesting from those engaged in Iran business, and certain states, including California and Florida, have implemented state laws prohibiting state government contracts with companies investing in Iran's energy sector (see, *WorldECR* issue 4).

Available sanctions

Sanctions available under the ISA

Denial of Export-Import Bank loans, credits, or credit guarantees for U.S. exports

Denial of licences for the export of military, dual-use, or nuclear-related goods or technology

Denial of U.S. bank loans exceeding $10m in any 12-month period

Prohibition on service as a primary dealer in U.S. government bonds, and/or prohibition on serving as a repository for U.S. government funds, if the sanctioned party is a financial institution (each counts as one sanction)

Prohibition on U.S. government procurement from the sanctioned party

Restriction on imports from the sanctioned entity

Sanctions now available under CISADA

Prohibition on foreign exchange transactions subject to U.S. jurisdiction

Prohibitions on banking transactions subject to U.S. jurisdiction

Prohibitions on transactions with respect to any property subject to U.S. jurisdiction in which the sanctioned party has an interest

Mandatory investigations and the enforcement of CISADA

Critics of the sanctions in place prior to CISADA questioned the level of discretion left to the President in determining whether to investigate activities that could trigger sanctions. The ISA stated that the President 'should' investigate potentially sanctionable activity, but the ISA did not require an investigation. CISADA represents a significant change in that it amends the ISA to require that the President investigate activities that could potentially violate the act's prohibitions.

President Obama delegated his authority to investigate potential violations of the ISA as amended by CISADA to the Department of State in a presidential memorandum dated 23 September 2010 (through which the President also delegated other authority under CISADA to both the departments of State and Treasury). Investigations are being handled by the Office of Terrorism Finance and Economic Sanctions Policy ('OTFESP'). Some members of Congress have lamented the lack of resources in the OTFESP and delays in the investigation process. Others have expressed frustration over the office's apparent failure to initiate investigations into certain companies publicly suspected of having engaged in sanctionable activities.

However, the administration has taken a number of actions to enforce

CISADA. On 30 September 2010, the State Department announced that Naftiran Intertrade Company, a Swiss company owned by National Iranian Oil Company, would be the first entity sanctioned under CISADA. The State Department then sanctioned Belarusneft, a state-owned Belarusian energy company, in March 2011 for having entered into a $500m contract with Naftiran to develop an oilfield in Iran. On 24 May 2011, the State Department announced sanctions against seven companies under CISADA: PCCI, Royal Oyster Group, Speedy Ship, Tanker Pacific, Ofer Brothers Group (later clarified to list specific members of the group), Associated Shipbroking, and Petroleos de Venezuela ('PDVSA') for shipping transactions involving refined petroleum products. These May 2011 sanctions represent a significant development given that they targeted companies providing shipping services and not just companies investing directly in Iran's energy sector, providing an example of the extended reach of sanctions under the ISA as amended by CISADA.

The administration has also used its authority under CISADA to persuade companies to wind down business with

Impact on business – new compliance considerations

As we wait to see whether the Obama administration will take further actions under CISADA, companies should evaluate their own compliance and susceptibility to CISADA sanctions. Because the sanction 'triggers' under CISADA now include assistance in the construction, modernization or repair of petroleum refineries as well as less direct contributions to Iran's refined petroleum industry (such as the supply of equipment and technology, insurance or reinsurance services, financing or brokering services, and the supply of ships and shipping services), the sanctions could impact companies and industries one or two steps removed from the energy sector. For example, transportation and shipping companies, logistics providers, industrial equipment and machinery producers, infrastructure development companies, consultants and other service providers should examine their customer base, analyze the potential uses of their goods, services, or technologies, and consider the potential impact of the CISADA sanctions on their business. Given the reach of the sanctions available to the President under CISADA, even companies with no U.S. business should take proactive measures to ensure their activities are not sanctionable.

Companies can take various steps to avoid engaging in sanctionable activities under CISADA. Generally speaking, this calls for increased due diligence in undertaking new business. Entities operating in the energy sector or providing construction, maintenance or other services to that sector should weigh the full scope of their activities against the list of activities that could trigger sanctions. Companies outside the energy sector should also analyze the extent to which supply of their products or services, even general use goods, such as pipes, valves, pumps, power generation systems, and other significant machinery and equipment, could potentially trigger sanctions. Logistics companies, insurance and other financial services providers, for example, should take active steps to understand their customers' business. It is often difficult for such companies to know the types of goods or services that could serve to enhance Iran's petroleum refineries or Iran's ability to import refined petroleum, but through active efforts to know their customers, such companies can reduce the risk of engaging in activities that could be considered to be sanctionable.

Implementing clear written internal policies and procedures can also help mitigate risk. CISADA provides that no sanctions are to be imposed on underwriters, insurers, or reinsurers that exercise due diligence in establishing and enforcing official policies, procedures and controls that aim to ensure compliance with the prohibition on support to Iranian imports of refined petroleum products. This exception suggests that, at minimum, companies, including those outside the insurance and re-insurance industries, would be wise to have such compliance controls in place. Companies should also consider adopting business practices that further protect against potential violations. The State Department, for example, encourages the use of coverage exclusions in insurance policies for losses associated with the delivery of refined petroleum products. Similarly, shipping associations have suggested employing contractual language that allows ship owners to refuse to deliver refined petroleum cargoes to Iran. These types of contractual provisions help protect such service providers from the risk of engaging in sanctionable activity, and similar approaches can be developed for other sectors and types of business.

Lastly, after identifying activities that are or may be sanctionable under CISADA, companies should weigh the benefits of approaching the State Department, OTFESP, under the 'special rule' to clarify the permissibility of the activities, and, if necessary, negotiate a winding-down of any operations of concern and avoid the business and reputational costs of a State Department investigation and potential subsequent sanctions. It is generally understood that companies may be permitted to fulfil existing contractual obligations, but the detailed nature of such obligations will have to be presented to the U.S. government. Indeed, companies availing themselves of the special rule are encouraged to provide a detailed catalogue of their existing activity in Iran as well as their plan for winding down any sanctionable activity as soon as possible. Companies with U.S. affiliates, or even companies that merely employ U.S. persons or have U.S. board members, will need to be comfortable that these U.S. persons have not been engaged in activities related to Iran that would constitute violations of the generally applicable Iran sanctions administered by the Office of Foreign Assets Control ('OFAC'), and, if necessary, address potential OFAC regulatory concerns prior to or concurrent with any approach to the State Department.

Iran. In fact, several companies have avoided investigation by the Obama administration because of the 'special rule' in CISADA that allows the President to decline to investigate companies that agree to wind down prohibited activities and certify that they will no longer engage in such activities. On 30 September 2010, for example, the State Department announced that Royal Dutch Shell PLC of the Netherlands, Total SA of France, Statoil ASA of Norway and ENI SPA of Italy had all agreed to take advantage of the special rule and cease prohibited activities involving Iran. A fifth company, INPEX of Japan, similarly pledged to end its sanctionable activities in Iran in exchange for avoiding investigation.

Additionally, the State Department reports that several companies have voluntarily decided to stop business with Iran since implementation of CISADA, including Turkish refiner Tupras, Kuwait's Independent Petroleum Group, India's Reliance, Malyasia's Petronas, Russia's Lukoil and Swiss energy traders Vitol, Glencore, and Trafigura. Repsol, BP, South Korea's GS Engineering & Construction and the German firm Linde have abandoned ongoing development projects or promised to forego planned participation in future projects, and Germany's ThyssenKrupp has gone a step further and offered to freeze all new business with Iran, even business outside the energy sector. Major insurers, such as Lloyd's of London, have stopped covering shipments of refined petroleum to Iran. Hong Kong shipping company NYK Line Ltd. has decided to withdraw from all trade with Iran.

Despite this flurry of activity over the past year, pressure is increasing on the Obama administration to do more. It is not clear that the sanctions have significantly disrupted the Iranian regime's efforts to obtain nuclear weapons. Moreover, while certain companies have been targeted by the administration, other suspected violators have not been investigated. Members of Congress, for example, have identified potential violators and inquired about such entities with the President, yet it is unclear whether such companies have been investigated. Similarly, a letter co-signed by 92 U.S. senators was delivered to the administration in August 2011 urging the President to sanction the Central Bank of Iran ('CBI'), using CISADA or other authorities available to him. There is growing frustration in the Congress over the administration's lack of action with respect to the CBI.

Increased enforcement and additional sanctions likely

The pressure on the Obama administration is increasing with respect to Iran, and frustration with the Iranian regime is growing in Washington, particularly following the news of its alleged involvement in a plot to assassinate the Saudi Ambassador. The Senate Committee on Banking, Housing & Urban Affairs held a public hearing on 13 October 2011 to discuss implementation of the CISADA sanctions with Obama administration officials. The House Foreign Affairs Committee followed suit on 14 October. During testimony before both committees, David Cohen, the Under Secretary of the Treasury for Terrorism and Financial Intelligence, indicated that 'all options' remain on the table for increasing financial pressure on the Iranian regime, including the CBI sanctions requested by 92 senators. Members of Congress continue to press not only for sanctions against the CBI but for an increase in the number of investigations of foreign banks and companies, additional designations of Iranian human rights abusers, and further efforts to pressure the European Union and other allies to stop purchases of Iranian crude oil.

While CISADA has had an impact on Iran's ability to develop its petroleum industry, the impact has done little to assuage concerns in the United States about Iran's efforts to develop a nuclear programme.

Legislation has been introduced in the Senate that would define what constitutes 'credible information' requiring initiation of an investigation, and would explicitly require the President to take action with respect to entities potentially engaged in sanctionable activity and identified in written requests by members of Congress. Senator Robert Menendez (D-NJ) has proposed legislation that would prohibit EU refiners from using Iranian crude oil in gasoline exported to the United States, while senator Jon Tester (D-MO) has asked the administration to close a 'loophole' and consider enforcing the more general OFAC-administered IEEPA-based Iran sanctions against foreign subsidiaries of U.S. companies, though such a change would likely require legislation to amend IEEPA and such efforts have failed in the past. For its part, the administration is engaged in diplomatic efforts to persuade countries like China, Spain, Japan, South Korea, India and Turkey to limit business with Iran's energy sector.

While CISADA has had an impact on Iran's ability to develop its petroleum industry, the impact has done little to assuage concerns in the United States about Iran's efforts to develop a nuclear programme, its support for terrorist groups, and human rights abuses. Given the continuing pressure on the administration, further actions under CISADA against companies engaged in business related to Iran are expected, and additional development or expansion of the overall U.S. sanctions regime remains a distinct possibility.

Jason Waite is a partner in the law firm of Alston & Bird in Washington, DC. He counsels clients on all aspects of export controls and economic sanctions, with an emphasis on compliance, transactional planning, and enforcement defense.
Jason.Waite@alston.com

Diego Marquez is an associate in the firm who specializes in international trade and regulatory compliance matters and represents clients' public policy interests before Congress and the administration.
diego.marquez@alston.com

Casting a wide net: China's encryption restrictions


While many governments are concerned about the exportation of high-level encryption technology and products and their subsequent use overseas, China's focus is on the use of encryption within its borders. Christopher T. Cloutier and Jane Y. Cohen examine the PRC's broad encryption controls.

China's web of encryption regulations has the potential to ensnare unsuspecting foreigners using their laptops or mobile phones in country. Under the Regulations for the Administration of Commercial Encryption ('Encryption Regulations'), adopted in 1999 by China's State Council – the highest organ of the state – the manufacture, use, sale, import, or export of any item containing encryption without prior government approval may lead to administrative fines, the seizure of equipment, confiscation of illegal gains, and even criminal prosecution.

The manufacture, use, sale, import, or export of any item containing encryption without prior government approval may lead to administrative fines, the seizure of equipment, confiscation of illegal gains, and even criminal prosecution.

The Encryption Regulations are written broadly, covering essentially any encryption product or technology used outside of official government channels. Starting shortly after these regulations were issued, there have been a series of statements by Chinese officials explaining that they are not intended to capture mass-market products that have only ancillary encryption functions, as opposed to dedicated encryption hardware or software. A clarification issued by one government agency in 2000, for example, explained that mobile phones, internet browsers, and Microsoft Windows software were not within the ambit of the Encryption Regulations.

Although thousands of individuals carry laptop computers and smartphones in and out of China every day, it is not without risk. To begin, the government statements that the Encryption Regulations are not intended to address standard, mass-market products have all been issued by entities subordinate to the State Council. Thus, these statements did not amend the Encryption Regulations but rather indicated how the government intends to enforce them. Such intentions can change quickly. In addition, most of the statements are now more than a decade old and do not necessarily reflect current conditions. The statements were, for example, issued well before the first smartphones hit the market, and before many companies began routinely adding specialized security software to computers issued to employees. Many of the more advanced features available in smart phones and security software installed on modern laptop computers would appear to be the type of technology that the Encryption Regulations seek to control.

China's encryption controls

The State Cryptography Administration ('SCA'), sometimes referred to by its former name, the State Encryption Management Bureau ('SEMB'), serves as the national authority responsible for the regulation of encryption products and technologies in China. The SCA formulates, adjusts, and publishes relevant rules and regulations. Together with the General Administration of Customs, the SCA also enforces China's restrictions on the importation of encryption products and technologies.

As indicated above, the Encryption Regulations are extremely broad. They restrict the development, production, sale, use, and even repair of commercial encryption products. Moreover, the Encryption Regulations severely limit the sale of foreign-made commercial encryption products in China. Specifically, the Encryption Regulations mandate that only SCA-authorized entities are allowed to sell SCA-approved encryption products in China. Both the importation and exportation of commercial encryption products and equipment containing commercial encryption technologies must be approved by the SCA. Foreign organizations, non-Chinese foreign nationals in China, including short-term visitors, are required to obtain a licence from the SCA before using any encryption product in China. Diplomatic organizations are specifically exempted.

Unlike U.S. export controls on encryption, which are increasingly streamlined to ensure that only sensitive types of high-level encryption items are captured, China casts a much wider net. In fact, article 2 of the Encryption Regulations clarifies that all 'encryption technologies and encryption products used for encrypting protection or security authentication of information' are covered to the extent that they are not used for national security purposes. Thus, the Encryption Regulations are broad enough to cover virtually any cryptographic technology or process, regardless of encryption strength or prevalence of a product in international markets.

The SCA has published a number of rules outlining controls on encryption

products in China. These rules include the following:

- *Rules on the Production of Commercial Encryption Products* (11 December 2005) stipulate that encryption products must only be manufactured by firms authorized by the SCA, and that the types and categories of encryption products to be produced must be approved by the SCA. In addition, manufacturers of encryption product that engage in government procurement activities must submit encryption keys to the SCA.

- *Rules on the Sale of Commercial Encryption Products* (11 December 2005) require a seller to obtain a sales licence for commercial encryption products prior to selling encryption products in China. Thus, encryption products developed or manufactured outside of China must not be sold in China without prior authorization from the SCA.

- *Rules on Scientific Research for Commercial Encryption Products* (11 December 2005) stipulate that R&D activities related to encryption products must only be conducted by entities authorized by the SCA.

- *Rules on the Use of Commercial Encryption Products* (24 March 2007) (the 'Use Rules') govern the use of encryption products by Chinese persons including FIEs ('foreign invested enterprises', *i.e.* Chinese-incorporated branches of foreign companies). The Use Rules provide that Chinese citizens and enterprises may use SCA-approved encryption products made in China without a licence. These SCA-approved encryption products are, however, only available through authorized channels, which allows the Chinese government to control their distribution. The Use Rules also provide that FIEs may apply for a licence to use foreign-made encryption technology or equipment given a demonstration of necessity.

- *Measures on the Use of Commercial Encryption Products in China by Foreign Organizations and Individuals* (24 March 2007) (the 'Foreign Organization Measures') regulate the use of encryption products in China by foreign persons including natural persons and 'organizations established under foreign laws outside the territories of China'. Thus, these rules apply to employees of companies visiting China who are not Chinese citizens. The Foreign Organization Measures require foreign persons using essentially any encryption products or technologies in China to obtain licences from the SCA.

- *Trial Measures on the Implementation of Commercial Encryption Administrative Punishments* (1 August 2007) regulate the actions of administrative authorities such as the SCA and relevant provincial and local encryption administration authorities.

- *The Import Control Catalogue of Encryption Products and Equipments Containing Encryption Technologies* (10 December 2009) lists the following nine controlled encryption products and equipment:

Encryption licence application procedures

For Chinese persons

Chinese persons including Foreign Invested Enterprises ('FIEs') may apply for a licence for virtually all activities involving encryption products, including the sale, use, import, or export of encryption products at the State Cryptography Administration ('SCA') branch office nearest where the applicant is located. The application packet must include a complete Registration Form For The Use Of Foreign-Produced Encryption Products and certain other documents such as business licences and a description of the encryption products to be licensed.

Review by the local SCA office lasts for five business days, at the end of which the application is either forwarded to the SCA in Beijing for further review or returned to the applicant for revisions. Review by the SCA in Beijing may last for up to 20 working days. If the application is approved, the SCA will issue a Certificate For Using Foreign-Produced Encryption Products, which is valid for three years. If requested, the SCA will also issue an Import Licence For Encryption Products, valid for 30 days. If the application is rejected, the SCA will provide the applicant with a statement of the reasons for the rejection.

For non-Chinese persons

The application process for non-Chinese entities is similar to that for Chinese persons. Applications must be filed with a nearest branch office of the SCA. For example, a foreigner wishing to import or use an encryption product in Guangdong Province would file the application with the Guangdong SCA. An application packet must also include a Registration Form For The Use Of Encryption Products By Foreign Organization And Individuals and certain additional documents such as business licences and a description of the encryption products to be licensed. Furthermore, if a non-Chinese entity wishes to use an encryption product that needs to be imported, then the importation of foreign encryption product requires a separate import licence, the application for which appears at the bottom of the Registration Form For The Use Of Encryption Products By Foreign Organization And Individuals. Notably, a frequent business traveller easily could fall foul of these provisions because each visit and importation into China of a particular encryption item (e.g. a laptop or a smartphone with encryption technology) could require a separate licence from the SCA.

Time periods for review of the application are the same as those discussed above for Chinese persons. Also as above, if the application is approved, the SCA will issue a Certificate For Using Encryption Products By Foreign Organizations And Individuals, which is valid for three years. If requested, the SCA will also issue an Import Licence For Encryption Products valid for 30 days. Rejected applications will be returned with a statement of reasons for the rejection.

- 8443311010: Electrostatic-sensitive multifunctional integrated encrypting fax machines (with automatic data processing equipment or network connection);
- 8443319020: Other multi-functional integrated encrypting fax machines (machines with the function of printing, copying or both);
- 8443329010: Fax machines (can be connected to automatic data processing facilities or internet);
- 8517110010: Cordless encrypting telephones;
- 8517180010: Other encrypting telephones;
- 8517622910: Optical communication encrypting routers;
- 8517623210: Non-optical communication encrypted exchangers;
- 8517623610: Non-optical communication encrypting routers; and
- 8543709950: Password machines (including telephone password machines, fax password machines, etc.), password cards.

Importantly, importers must apply for an import licence when importing into China any of the aforementioned products, as well as other products which the importer 'knows or should know' contain 'encryption technologies', including those not specifically enumerated in the catalogue.

Under some circumstances, leasing of encryption items in China may be more advantageous.

PRC encryption enforcement

The SCA itself does not have enforcement powers and must rely on other Chinese government agencies. Such agencies include the General Administration of Customs, Public Security Bureau, State Security Bureau, Administration for Industry and Commerce, and the Administration for the Protection of State Secrets. Recent developments indicate that these agencies plan to take a more active role in enforcing China's encryption controls. Thus, persons who engage in activities in China involving encryption products (*e.g.* the importation and use of encryption products), without complying with the existing rules should focus on taking the necessary steps to bring themselves into compliance with China's encryption controls or face potential enforcement actions and penalties.

To ease the licensing burden and reduce the risk of falling foul of Chinese encryption laws, persons that engage in activities in China should consider activities that involve unencrypted laptops, smartphones, and other unencrypted electronic devices. However, the obvious disadvantage to this approach is the decreased data security resulting from the lack of encryption.

Under some circumstances, leasing of encryption items in China may be more advantageous. Although this approach would avoid having to obtain, for example an import licence in advance of each trip to China, a three-year 'use' licence would still be required. Obtaining a 'use' licence could be averted altogether if a company that leases encryption products to third parties already has the necessary 'use' licences for its encryption items.

Special thanks to Michelle Yingjie Li, an international legal consultant with King & Spalding's Washington office, for her assistance with this article.

Persons involved in the drafting this article are not licensed to practise law in China.

Christopher T. Cloutier is a partner and Jane Y. Cohen an associate in the Washington, DC office of King & Spalding LLP.
ccloutier@kslaw.com
jcohen@kslaw.com

Pole position


Businesses trading in Poland are obliged to follow national permitting procedures or incur criminal or administrative penalties. Emilia Stępień and Krzysztof Korwin-Kossakowski provide an introduction to Poland's export control regime.

As a Member State of the European Union, Poland is subject to the provisions of EU Regulation No 428/2009 on setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items (the 'Regulation'). The Regulation provides for its implementation in the Member States. In Poland it is implemented by the Act of 29 November 2000 on foreign exchange in goods, technologies and services of strategic importance for national security and for maintaining international peace and security (the 'Act') and related by-laws. The Act and related by-laws concern items of strategic importance (the 'Items'). The Items include:

- dual-use items as defined in the Regulation, and
- military items that are not covered by the Regulation.

Dual-use items are items, including software and technology, which can be used for both civil and military purposes. They include all goods which can be used for both non-explosive uses and which in any way assist in the manufacture of nuclear weapons or other nuclear explosive devices. Military items are weapons, ammunitions, explosives and technologies that are specified on a military items list. The Items are listed

- as regards dual-use items in the regulation of the Minister of Economic Affairs of 2 October 2002 on the list of items of strategic importance. The list reflects the list of items in attachment No. I of the Regulation;
- as regards military items in the regulation of the Minister of Economic Affairs of 1 February 2011 on the list of military items, of which trading is subject to a permit.

Trade under the Act covers export, agent services, technical support, import, transit (the 'trade'). Thus, the Act regulates a wider scope of activities than the Regulation. The trade is subject to exporters' regulatory obligations (including relevant permits and notifications) and control.

Import is understood as introducing Items into Poland or transmitting information, documentation or software with the use of electronic means of communication, from a third country to Poland.

Technical support is understood as any technical support connected with amending, developing, producing, testing, maintaining and other technical services concerning Items.

The Act of 29 November 2000 on foreign exchange in goods, technologies and services of strategic importance for national security and for maintaining international peace and security regulates a wider scope of activities than EU Regulation No 428/2009.

The Act applies to all individuals, legal persons or partnerships wishing to trade with Items. Natural and legal persons localized in Poland who wish to export Items to a third country are further called the 'exporter', and natural and legal persons localized in Poland who wish to import Items from third countries are further called the 'importer'.

The Minister of Economic Affairs is appointed as the authority responsible for controlling exports (the 'Control Authority'). The Control Authority is authorized to appoint a team (the 'Team') to which certain export-controlling task are delegated. The customs control of Items is conducted only by specified custom offices.

Permits

Trade with Items may be subject to a permit. The permit to trade with the Items is granted by the Control Authority. Exporters granted a permit cannot assign it to another entity and may only exercise the permit themselves. The permit must indicate the scope of lawful trade and trading with Items outside the scope of the permit is unlawful. Applying for the permit as well as its issue is free of charge.

Dual-use items

A permit governing trade in dual-use items is required for:

- export,
- other services (i.e., brokering services, transit, forwarding, and technical services).

There are three types of national permits for trade with dual-use items:

a) individual
b) general; and
c) global.

In addition, exporters from Poland may trade with dual-use items on the basis of a general permit covered by the Regulation. The Act does not define the scope of permits so the Regulation is directly applicable.

General permits

The general permit is granted by statute and may be used by all exporters who meet the requirements

therein. Exports based on these permits can only be made to states listed in the statute, and include listed items. Exporters may use the general permits when they:

- can prove compliance with internal trade control standards for a period of at least three years prior to having relied on the general permit; and
- notify the Control Authority that they would like to start trading with Items covered by the permit.

Individual and global permits
The individual permit is for a specific exporter who intends to export one or more Items to one specific end-user. The global permit is for a specific exporter who intends to export Items to one or more specified end-users in one or more specified third country.

Individual and global permits are granted by the Control Authority, upon application by the exporter. The permits are granted to exporters complying with the conditions described below.

In the application for an individual or a global permit, the exporter must provide certain information such as the destination of the Items, the end-user and so on. Exporters should also attach to the application the import certificates (with a sworn translation) from the respective authorities of the end-user's country.

Exporters are obliged to investigate how the end-user intends to use the Items and ensure that the end-user does not intend to use the Items for:

(i) suppression or violation of human rights
(ii) threatening world peace or destabilising a certain part of the world
(iii) supporting terrorism; or
(iv) any use other than one justified by the need to maintain the safety and security of a state.

Import of dual-use items
Although the importing of dual-use items to Poland is not subject to import permit as such, some dual-use items are monitored. This is the case with any dual-use items used in telecommunications and information security. In practice, it means that the importer of such dual-use items must notify the Director of the Internal Security Agency (the 'Monitoring Authority') of the envisaged import.

That notification should be submitted 14 days prior to the envisaged import, and should include:

(i) the importer's details
(ii) details of the person who is supposed to receive the imported items
(iii) details of the producer of the Items
(iv) information as to how the Items are going to be used
(v) details of the end-user's country
(vi) the declaration that the Polish importer ensures the Items will reach the declared end-user.

Military items
Trade in military items may only be conducted based on an individual permit which may be granted for:

- export
- import
- other services (that is brokering services, transit or forwarding, technical services).

In order to obtain an individual permit to trade with military items, the exporter needs to meet the same conditions as those required to obtain an individual permit to trade with dual-use items as listed above.

Controls
Controls may cover all activities that fall under the definition of trade. Control activities are undertaken both by the exporters and the Control Authority.

Control before granting the permit
Internal control system
Exporters are obliged to set up an internal control system prior to

Penalties

An exporter may be liable to criminal or administrative sanctions for breach of Polish export control law.

Criminal penalties may be imposed:

(i) for exporting Items without an appropriate permit. The exporter (the exporter being a natural person as well as being a legal person, and its managing directors) may be liable to a fine, restriction of freedom or imprisonment of up to ten years. If the exporter's acts were unintentional, the exporter may be subject to a fine, restriction of freedom, or imprisonment up to two years.
(ii) on an exporter (that is individual or managing director of exporter being legal person) who:

a. does not apply for a Customs Certificate,
b. obstructs control, or
c. fails to notify the import in dual-use items.

In such a case, the exporter may be liable to a fine.

Administrative penalties that may be imposed on exporters (except where they are natural persons) include:

(i) for trading with Items without a proper permit, a penalty of up to 200.000 PLN (approx. 45,00.00 EUR);
(ii) for importing Items without notifying the Monitoring Authorities, a penalty of up to 100.000 PLN (approx. 22,500.00 EUR);
(iii) for trading with Items beyond the scope of the permit, a penalty of up to 100.000 (approx. 22,500.00 EUR);
(iv) for not applying for a Customs Certificate, a penalty of 50.000 (approx. 11,250.00 EUR).

Penalties should be paid within 30 days from the date when they were imposed and will be. Such penalties are void after five years.

applying for a permit. The internal control system should cover:

- internal processes
- the structure of the exporter's enterprise, the employees and the management.

The internal control system is subject to certification by the respective national certifying authorities. It is controlled by the Control Authority before the permit is granted.

Catch-all rule
Exporters trading with Items are obliged to verify the destination and use of the military items (the so-called 'Catch-all' rule). This means that the exporter should always take utmost care when undertaking the trade and, itself, check:

- what the destination of Items really is
- whether the use of Items can be a threat to national peace
- whether the end-user's country supports terrorism etc.

If the exporter is unable to appropriately verify the real destination of Items and their use, the exporter can request a binding opinion from the Control Authority as to whether the trade is a threat the peace.

Records
Exporters are obliged to keep records of their trade in Items. Additionally, exporters using a general permit are obliged to notify the Control Authority, at least every six months, of trade undertaken and the country of destination.

Controls after the granting the permit
Exporters are subject to controls after the permit has been granted. This includes:

- verification of transactions subsequent to their conclusion (and to their compliance with the scope of the permit)
- verification of the internal control system
- verification of the record of transactions.

This verification control may be performed by the Team, which is entitled to enter the exporter's premises, demand oral or written explanations, documents, data files and other information related to the Items and transactions. The control is undertaken in the presence of the exporter.

If the control reveals any violations of the Act, the exporter has a month to comply with the Polish export control law and the terms of the permit. If the exporter fails to comply, the Control Authority may revoke the permit (in the case of individual and global permits) or prohibit the use of a general permit. The exporter may only apply for a new permit three years after having the permit revoked.

Other control measures
The Act obliges exporters to obtain permits for any exports which, though not listed as Items, are to the exporter's best knowledge, destined to be used as part of a weapon.

If the exporter is unable to appropriately verify the real destination of Items and their use, the exporter can request a binding opinion from the Control Authority as to whether the trade is a threat the peace.

Import certificates
Under the Act, the Control Authority may, upon an exporter's application, issue an import certificate or confirm the importer's statement that Items have a specific destination. A certificate or statement may be required by the third parties' authorities.

It is worth noting that Polish law requires the exporter of the Items to provide an import certificate issued by the foreign country's authorities or a statement of the end-user confirmed by those authorities.

After the release of Items from Polish customs, foreign exporters granted an import certificate must acquire confirmation from the respective Polish customs office certifying that the Items have been in fact and lawfully imported into Poland ('Customs Certificate').

Refusing/revoking the permit
The Control Authority must refuse the grant of a permit if:

(i) it is a requirement of national safety and defence of Poland
(ii) such are obligations of Poland deriving from international treaties
(iii) the exporter applying for permit does not give a guarantee that he will observe Polish law
(iv) the Items are destined to be used for illegal purposes or purposes contradictory to Polish reason d'état.

The Control Authority may refuse to grant a permit if:

(i) it is possible that the destination of the Items may be changed or
(ii) the exporter has already violated the law on trade in Items.

Exporters must at all times observe Polish export control law. Where the Control Authority discovers that an exporter has failed to observe his obligations, the Control Authority must refuse to grant the permit or may revoke it. The reasons for revoking the permit are analogous to those for refusing to grant it.

The Control Authority is authorized to revoke the permit only after acquiring the opinions of the Minister of the Foreign Affairs, the Minister of Defence, the Minister of Internal Affairs, the Director of the Internal Security Agency, the Head of the Intelligence Agency, and the Minister of Finance.

Emilia Stępień is a senior associate and Krzysztof Korwin-Kossakowski a junior lawyer at Bird & Bird LLP's Warsaw office.
emilia.stepien@twobirds.com
krzysztof.korwin-kossakowski@twobirds.com

SMi
LINKING BUSINESS *with* INFORMATION

SMi present their inaugural....

DEFENCE EXPORTS ASIA-PACIFIC

1st and 2nd February 2012
Grand Copthorne Waterfront Hotel, Singapore

JUST ANNOUNCED:

MASTERCLASS:

Tuesday 31st January 2012, 13.30-17.00

Critical Success Factors in the development of an Offset programme

Led by: David Hew, Lawyer, APCA

APCA | OFFSET COUNTERTRADE STRUCTURED FINANCE

KEY SPEAKERS INCLUDE;

Ambassador Sune Danielsson, Head of Secretariat, **Wassenaar Arrangement**

Angelina Gurunathan, Principal Assistant Director, **Ministry of International Trade and Industry (MITI), Malaysia**

Ian Stewart, Advisor to the British Government's Export Control Process on the role of the Private Sector in Countering Proliferation, **King's College London**

James Hursch, Director of the Defence Technology Security Administration (DTSA), **U.S. Department of Defense**

James Yang, Deputy Executive Secretary, Export Control Task Force, **Bureau of Foreign Trade, Taiwan**

Kevin Wolf, Assistant Secretary for Export Administration, **U.S. Department of Commerce**

Mohamed Shahabar Abdul Kareem, Strategic Trade Controller, Strategic Trade Secretariat, **Ministry of International Trade and Industry (MITI), Malaysia**

Naeem Azid, Director, Licensing and Regulations, Strategic Export Control Division, **Ministry of Foreign Affairs, Pakistan**

Robert. S. Kovac, Managing Director, Directorate of Defence Trade Controls, **U.S. Department of State**

Tran Ba Cuong, Director of Origin and Control Division, **Ministry of Industry and Trade, Vietnam**

REASONS TO ATTEND:

- **MEET** senior policy makers from the Asia-Pacific region
- **DISCUSS** the latest regulations and export controls across Asia
- **ANALYSE** the most recent reforms to the ITAR and EAR
- **ASSESS** the latest regulations in the Asia-Pacific region
- **LEARN** which new treaties have been introduced in the Asian market
- **REACH OUT** to senior representatives from the U.S. Departments of Commerce, Defense and State
- **NETWORK** with senior policy makers

Sponsored by

COVINGTON
COVINGTON & BURLING LLP

pillsbury

PLUS 2 HALF-DAY POST-CONFERENCE WORKSHOPS
Friday 3rd February 2012, Grand Copthorne Waterfront Hotel, Singapore

Export Controls in Europe

08.30 – 12.30

Workshop Leader: **David Hayes,** Director, **David Hayes Export Controls**

In association with: David Hayes EXPORT CONTROLS

IT Challenges in Effective Export Control Compliance?

13.30 – 17.30

Workshop Leader: **Gary Stanley,** President, **Global Legal Services**

In association with: GLOBAL LEGAL SERVICES

Register online at www.defence-exportsasia.com

Alternatively call +65 664 990 95/96 or +44 (0) 870 9090 711

CPD CERTIFIED
The CPD Certification Service

Germany: dual-use controls

German regulations governing the export of dual-use items

While Germany's national trade legislation mainly serves to implement European provisions and to create correspondent rules of procedure, it does provide scope for specific national law. Holger Schmitz examines the key elements of the country's national legislation controlling the export of dual-use items.

Germany's national legislation dealing with foreign trade is predominantly laid down in the Foreign Trade and Payments Act (*Außenwirtschaftsgesetz* – hereinafter referred to as 'AWG'); the German Regulation Implementing the Foreign Trade and Payments Act (*Außenwirtschaftsverordnung* – 'AWV'); and the German Export List (*Ausfuhrliste* – 'AL') as an annex to AWV. However, section 1(2) AWG explicitly stipulates that European law on foreign trade takes precedence over respective national legislation. Since Council Regulation (EC) No 428/2009 on dual-use items ('REG') establishes a comprehensive foreign trade regime for dual-use items, most provisions which govern the foreign trade of dual-use items in Germany originate at European level. Thus, Germany's national legislation mainly serves to implement the European provisions and to create correspondent rules of procedure. In addition, it uses the (small) leeway allowed by REG to create rules applicable only at national level. Furthermore, Germany's national legislation sets out the sanctions which apply when 'dual-use provisions' are violated. This article mainly concentrates on the special features of Germany's national legislation in this area.

Licensing requirements

According to article 9(2) REG, export authorizations are to be granted by the competent authorities of the Member State where the exporter is established. Authorizations for intra-Union transfers must be applied for in the Member State from which the dual-use items are to be transferred (article 22(3) REG). As a consequence, in all these cases the German authorities are responsible for licensing – i.e. regardless of the origin of a licensing requirement (from European or German law). The competent German licensing authority is the Federal Office of Economics and Export Control (*Bundesamt für Wirtschaft und Ausfuhrkontrolle* – 'BAFA') which reports to the Federal Ministry of Economics and Technology (*Bundesministerium für Wirtschaft und Technologie*).

Germany's national legislation sets out the sanctions which apply when 'dual-use provisions' are violated.

Most licensing requirements for the shipment of dual-use items in Germany result from their entry in annex I REG since, according to article 3(1) REG, every export of a dual-use item controlled by annex I in principle requires authorization. Annex I can be found in identical form in part I section C of the German AL. The latter therefore does not for the most part establish any further licensing requirements. Only numbers 901 to 999 of part I section C AL, to some extent, comprise additional national items with a possible use for military purposes (such as land vehicles, transmitters or helicopters). As far as these items are concerned, section 5(2) AWV establishes a licensing requirement for items with a value exceeding 2,500 euros (cf. 5(3) AWV).

The export of items not controlled by annex I REG/AL may nevertheless require authorization if the items are or may be intended for sensitive purposes and are therefore covered by European or German catch-all clauses. Article 4 REG stipulates a licensing requirement if items to be exported

- are or may be used for sensitive purposes associated with ABC weapons (article 4(1) REG),
- are or may be intended for a military end-use of any kind if the country of destination is subject to an arms embargo (article 4(2) REG), or
- are or may be intended for use as components of military items listed in the national military list exported without authorization (article 4(3) REG).

In Germany, article 4(3) REG applies to items listed in AL part I section A. In addition to article 4 REG, Germany has established catch-all clauses in sections 5c and 5d AWV. Section 5c AWV applies if military end-use is or may be intended (identical to Article 4(1) REG) and the country of destination is contained in Country List K (*Länderliste K* – at present, this includes Cuba and Syria). Section 5d AWV applies if the items are or may be intended for the setting-up, operation of, or incorporation into, a nuclear plant and if the purchasing country or country of destination is Algeria, India, Iran, Iraq, Israel, Jordan, Libya, North Korea, Pakistan or Syria.

With the exception of data-processing programmes (software) and technology, sections 5c and 5d AWV only apply for items with a value exceeding 2,500 euros (cf. section 5c (4) and section 5d (4) AWV). Both the licensing requirements under article 4 REG and sections 5c and 5d AWV are triggered either by notice from BAFA stating that a sensitive purpose may be intended or the corresponding awareness of the exporter who has to

Germany: dual-use controls

inform BAFA of such on the licence application form. BAFA then decides whether a licence is required.

According to article 22(1) REG, intra-Union transfer of dual-use items only requires authorization if such are listed in annex IV REG. However, article 22(2) REG stipulates the possibility for Member States to impose an authorization requirement for the transfer of other dual-use items if at the time of the transfer the operator knows that the final destination of the items concerned is outside the European Union. Germany has made use of this option in section 7(2) AWV. Furthermore, sections 7(3) and 7(4) AWV establish licensing requirements if the direct export to the country outside the European Union would be subject to article 4(2) REG or sections 5c and 5d AWV (i.e. the transferor is informed by BAFA about a sensitive purpose or aware of such).

According to article 5(1) REG, trafficking and brokering transactions related to dual-use items listed in annex I may require licensing if the broker has been informed or is aware that the items in question 'are or may be intended, in their entirety or in part, for any of the uses referred to in article 4(1)' REG. At German level, section 41 AWV establishes a corresponding rule for items listed in AL part C numbers 900 to 999 (dual-use items not listed in annex I to REG) 'that are located in a third country or the economic territory and have not been subjected to import clearance yet, and that are to be exported to another third country'. Section 41a AWV establishes a similar licensing requirement for trafficking and brokering transactions related to dual-use items listed in annex IV.

Regarding technical assistance related to dual-use items, licensing requirements may result from sections 45ff AWV, which apply under the conditions stated in article 4 REG, and 5c and 5d AWV (see above).

Types of licences

If a shipment licence is required, Germany offers several types. The (basic) individual licence permits shipment on the basis of one order to one consignee.

As a special form of individual licence, the maximum amount licence (*Höchstbetragsgenehmigung*) permits shipment based on several contracts (e.g., within a framework agreement) to one customer up to the approved maximum amount. A collective export licence (section 2 AWV – *Sammelgenehmigung*) may be granted to reliable exporters heavily involved in foreign trade. It is limited in time and permits several exports or transfers to several customers at several destinations as indicated in the licence. The applicant has to provide evidence of the reliability of the customers and must maintain an internal export control system (cf. *Collective Export Licence Information Leaflet* (*Merkblatt Sammelausfuhrgenehmigungsverfahren*) – at www.ausfuhrkontrolle.info).

A further type of licence of growing importance is the general export authorization. General authorizations exist at European and national level and exempt exporters/transferors from applying for individual approval as long as the envisaged transaction falls under the scope of the general authorization. Community General Export Authorization ('CGEA') No EU001 (as stated in annex II REG) covers the export to Australia, Canada, Japan, New Zealand, Norway, Switzerland and the USA of all dual-use items specified in any entry in annex I except those listed in part 2 of CGEA EU No EU001. Part 2 most notably mentions all items specified in annex IV. CGEA EU001 stipulates that exporters must notify the competent authorities of the Member State where they are established of their first use of the CGEA no later than 30 days after the date on which the first export takes place. Furthermore, it stipulates that Member States may define further requirements regarding registration and reporting duties. Germany has made use of this option with the Announcement on the use of Community General Export Authorization No EU001. After the

Applying for licences

Applications for licences need to be filed with the Federal Office of Economics and Export Control ('BAFA'). In cases of doubt regarding the classification of items (and the corresponding licencing requirement), exporters may file a preliminary enquiry (*Voranfrage*) to clarify whether an export requires, and is eligible for, a licence.

The product-related advice on the list of goods (*Auskunft zur Güterliste* – 'AZG') verifies to customs authorities that a certain item is not listed. BAFA maintains an electronic licensing system called ELAN-K2. Thus, the whole licensing process, as well as many parts of the related communication, is paperless. For every shipment requiring an application, exporters/transferors must enter their customs number (assigned by the Federal Customs Service – *Bundeszollverwaltung*) in the application form. In addition, most exports require the nomination of a person responsible for exports and compliance with the corresponding regulations. Furthermore, end-use documents must be enclosed with the application (cf. Section 17(2) AWV) for the export of items listed in Annex I REG/AL. The same is true for transfers subject to approval due to their listing (cf. Section 21 AWV).

End-Use Certificates are divided into Private End-Use certificates (*Private Endverbleibserklärung*); Official End-Use certificates (*Amtliche Endverbleibserklärung*); and International Import Certificates (*cf. Bekanntmachung über Endverbleibsdokumente nach § 17 Absatz 2 der Außenwirtschaftsverordnung* – visit www.ausfuhrkontrolle.info).

The Private End-Use Certificate contains the statement of a private end-user giving information about the items to be delivered, the final destination and the designated use of the items. The Official End-Use certificate contains a similar statement of a governmental end-user. An international import certificate is issued by certain countries and contains the declaration of the recipient country that the exported/transferred items and a potential re-export are subject to the recipient country's export control law after border crossing. If general authorizations apply, no End-Use Certificates need to be provided.

To allow BAFA the technical assessment (and classification) of the item to be exported/transferred, all relevant technical data has to be provided with the application.

Germany: dual-use controls

Guidance

BAFA (the Federal Office of Economics and Export Control), as the central licensing authority, provides guidance in several ways to facilitate the licensing process.

On its website, www.ausfuhrkontrolle.info, BAFA publishes important regulations as well as announcements and explanatory notes providing information about recent developments and guidance on the practical appliance of export regulations.

A comprehensive commentary on German export control including all relevant texts and forms can be found in the *Handbook of German Export Control* (*Handbuch der Deutschen Exportkontrolle – HADDEX*) published and regularly updated by BAFA in four loose-leaf volumes. Furthermore, the handbook Export Control Practice (*Praxis der Exportkontrolle*) provides guidance on in-house compliance with export control law.

The English version of BAFA's website contains brief guidelines on German export control and translations of key regulations (bafa.export_control/index.html).

notification of first use, exporters are assigned a registration number. From then on, every January and June every export in the previous six months has to be reported unless the export is covered by a specific German general export authorization (see below). An appropriate statement has to be issued if no exports are carried out.

Article 9(2) REG gives Member States the possibility to establish general authorizations on their part, if no European general authorization exists. Germany has made use of this possibility and has established 13 national general authorizations ('NGAs'). NGAs covering dual-use items are (details available at www.ausfuhrkontrolle.info):

- General Authorization No 9 on certain graphites
- General Authorization No 10 on Computers and related items
- General Authorization No 12 on the export of certain dual-use items not exceeding a certain value. This NGA permits the export of most items listed in Annex I REG if the export does not exceed a value of 5,000 euros.
- General Authorization no 13 on the export of certain dual-use items in certain cases. This NGA covers the export of items which serve predefined purposes.
- General Authorization no 16 on telecommunications and information security

Since article 9(2) REG stipulates that all national 'authorizations shall be valid throughout the Community' the above-mentioned NGAs may be used even if the items are not located in Germany but in another Member State.

The NGAs do not apply to exports to Australia, Japan, Canada, New Zealand, Norway, Switzerland and the U.S.A. since export to these countries is covered by CGEA EU001. Furthermore, they do not apply to exports to countries subject to an arms embargo under article 4(2) REG and countries explicitly designated in the particular NGA.

As for CGEA EU006, notification of first use within 30 days is required. Furthermore, NGA no 9 requires notification of the exports carried out. NGAs nos 12 and 13 require notification only for some of the covered items and NGAs nos 10 and 16 require no notification at all. However, if no notification is required, a report on the exported items has to be furnished on request (all documents relating to the usage of the general authorizations have to be kept for three years).

Since no fewer than seven Member States have NGAs in force, European exporters face unequal conditions.

No NGAs apply in the cases of article 4 REG or sections 5c and 5d AWV (i.e. the exporter is informed by BAFA about a sensitive purpose or is aware of it). NGAs nos 10 and 16 do not apply for certain encryption items if the exporter is aware that the purchaser or consignee is the military, paramilitary forces, the police, intelligence service or a civil administration acting for such institutions. If several NGAs apply, the exporter/transferor may choose between them.

Since many Member States do not have NGAs in force, European exporters face unequal conditions. To align and simplify the current system, the Commission proposed a council regulation setting up six new CGEAs (nos EU002 to EU007 – cf. COM (2008) 854 final). In its recently published Green Paper, 'The dual-use export control system of the European Union: ensuring security and competitiveness in a changing world' (COM(2011) 393 final), the Commission endorsed this initiative.

The new CGEAs (currently being negotiated) would be geared to existing NGAs and in some cases replace them (since the existence of CGEAs excludes the possibility of NGAs in the scope of the respective CGEA). This would notably be true for most German NGAs covering dual-use items. CGEA no EU002 on 'Low Value Shipments' would in some parts replace NGA no 12; CGEA no EU003 on 'Export after Repair / Replacement' would replace parts of NGA no 13; CGEA no EU005 on 'Computers and related equipment' would replace most parts of NGA no 10; and CGEA no EU006 on 'Telecommunications and Information Security' would in most parts replace NGA no 16.

Sanctions

Voluntary or negligent infringements of licensing requirements are considered as administrative offences (section 33 AWG) or criminal offences (section 34 AWG) and may result in severe punishments in the shape of fines or jail sentences.

Dr Holger Schmitz is a partner in the Berlin office of Noerr LLP. Holger co-heads the Regulatory and Governmental Affairs department of the firm.

holger.schmitz@noerr.com

ITAR rule change guidance for the UK

In October, the U.S. published a Q&A matrix on the implementation of ITAR rule change (76 FED REG 28174) concerning dual and third country national as guidance for the United Kingdom. We reprint the guidance with accompanying notes below.

Below we print a list of questions 'put to and answered by the US Department of State (DoS) (Director of Policy, Directorate of Defense Trade Controls) by HM Government (HMG) and UK industry, concerning this rule change which alters the way in which access by Dual and Third Country Nationals (DTCN) employees of importing (non-US) entities to ITAR-controlled material is controlled. The effective date of the rule was 15th August 2011.

'This UK-specific Questions and Answers Matrix has been agreed by DoS to help UK End Users and Consignees comply with the rule change requirements and complements the Technology Security Plan (TSP) that HMG has also agreed with DoS. The information suggested in this document is for guidance only and made without any endorsement, representation or warranty. It is not intended to provide legal or professional advice, and any party seeking to rely on it should ensure that it has obtained its own legal advice to ensure that it is applied in accordance with UK law.'

Key:
Clarification Question
DoS Clarification

1. Is ITAR 124.16 still available for use as an alternative to ITAR 126.18 in TAA and MLA?

Yes ITAR 124.16 is still available.

2. Does the new rule change offer two genuine alternatives to compliance by foreign consignees/end users; as employers they either obtain formal Government security clearance for their affected employees, or subject them to bespoke screening?

There are two genuine alternatives, ITAR 126.18(c)(1) and ITAR 124.18 (c)(2). The screening procedures and associated requirement only apply to the second, and not the first which is solely concerned with security clearance of employees.

3. What level of a formal Government Security clearance will suffice to meet the requirements of ITAR 126.18(c)(1)?

Any security clearance approved by the host Government of the end user/consignee is sufficient to meet these requirements. In the UK, Security Check (SC) clearance meets these requirements.

4. Does the new rule apply to the export of UNCLASSIFIED ITAR-controlled material only? What then is the position in relation to the export of classified material?

The ITAR 126.18 exemption is only available for UNCLASSIFIED US ITAR-controlled exports (below US CONFIDENTIAL). The US-UK Exchange of Notes (EoN) makes it clear that classified exports are to be dealt with separately under the UK-US General Security Agreement.

5. Does the new rule extend to all ITAR-controlled exports, or only to those governed by TAAs and MLAs?

The new rule applies to the export of all ITAR-controlled material and hence all forms of US arms export licence. DoS has recently published guidance on how to implement the new rule for licenses and Warehouse and Distribution Agreements.

6. Why does the scope of the new rule include technical data but exclude "defense services", even though both are encompassed by TAA/MLA?

"Defense services" cannot be retransferred as such. "Defense services" do however remain a feature of retained ITAR 124.16 (amended) for MLA/TAA.

7. How does the new rule treat sub-licensees and how do sub-licensing provisions work in relation to hardware licensing?

The new rule applies equally to sub-licensees as it does to licensees. It has no bearing on formal applications for re-transfer. For hardware licensing see 5 above.

8. Does conflict exist between ITAR 126.18 and ITAR 126.1(a), if so how will this be dealt with?

No conflict exists, because of the insertion of the phrase "notwithstanding any other provision of this part" into ITAR 126.18. "Part" here means Part 126. Hence the exemption applies to 126.1(a) nationals and dual nationals who have undergone the UK's Baseline Personnel Security Standard (BPSS).

9. How does the new rule apply to end users and foreign consignees? Is there a distinction?

The new rule applies equally to end users and foreign consignees wherever they operate.

10. Does the ITAR 126.18 requirement for NDAs (for employers with non-security cleared employees) apply to employers, employees or both?
How will this requirement work in relation to foreign governments and international organisations (NATO, EDA etc?)

Only the employer itself needs to enter into an NDA on a self-certification basis. Individual employees need not do so. This does not prohibit use of employee NDAs to support employer NDAs, but this is not an ITAR requirement and is a matter for the end user/consignee.

End users and consignees should note that the NDA required for the purpose of this rule change is not the same as the NDA referred to under existing Dept of State/DDTC Agreements Guidelines (Tab 11 refers).

HMG may follow the same process.

The NDA requirement does not apply to international organisations such as NATO and EDA.

11. What form should the NDA take?

A model NDA is to be found in the TSP and has been endorsed by DoS. This forms part of the agreed TSP for the UK and meets the NDA requirements for all exports. DoS have also confirmed that the NDA process will involve self-certification without any need for delivery to DoS.

12. Does the new rule permit transfers to employees outside of "the physical territories of the country where the end-user is located or the consignee operates"?

The transfer of defense articles pursuant to this section must take place completely within the physical territory of the country where the end-user is located, where the governmental entity or international organization conducts official business, or where the consignee operates, and be within the scope of an approved export license, other export authorization, or license exemption.

13. How does the rule apply to personnel within the UK's Armed Forces? Are these to be treated as "bona fide, regular employees, directly employed by the....foreign government entity" (ITAR 126.18 (a) refers)?

HM Armed Forces personnel are to be treated by the rule in the same way as other employees.

14. Will the new rule require or imply the use of certification by end users/foreign consignees to exporters, that they have screened their affected employees for risk of diversion?

No certification is required. Indeed certification should not be requested by exporters.

15. Does the rule require the disclosure of personnel records of employees of UK employers to DoS?

DoS understands that any disclosure must be in accordance with UK law. The EoN between the US and UK Governments recognises this and acknowledges the existence of previously agreed bilateral arrangements between the two Governments. Any disclosure requests by DoS or its agents will be made via HMG.

16. ITAR 126.1 cross-reference – Is it accepted that employees can travel for business, family and personal reasons?

Yes.

17. What about current employees who don't have Baseline Personnel Security Standard (BPSS) clearance?

Those affected employees already handling ITAR controlled materiel should already be covered under existing licences. Other employees will be covered when the consignee has a BPSS process in place.

18. Under ITAR 127.1(b), compliance obligations fall to the licensor. Is this still the case with ITAR 126.18?

This is not specifically addressed in the final rule change, but the answer is no. DoS guidance on their website makes it clear that licensors have no obligation to obtain written statements or certifications from foreign companies with regard to 126.18.

19. What about supply chains? How are UK primes to ensure compliance by their sub-contractors, including those across the EU?

There is no requirement to flow down ITAR 126.18 requirements to suppliers (sub-licensees). Each supplier must take responsibility for complying with ITAR 126.18 etc. Prior DDTC consent is still required for retransfers to third country suppliers.

20. To what extent, if any, could S 2(3)(B) of the Protection of Trading Interests Act 1980 render any discovery type activity by US authorities inadmissible?

There is no restriction on the UK Secretary of State's powers under the 1980 Act. The EoN makes it clear that exchange of information must adhere to applicable agreed bilateral US UK protocols. It will not therefore be necessary to invoke the PTIA.

21. Is HMG content there are no conflicts with national regulations on employment law, privacy law etc?

It is for each end user/consignee to ensure that their implementation of the rule change is effected in a manner which complies with UK law. The TSP, model NDA and this Q&A Matrix are provided as guidance to assist end users/consignees in this exercise, but in the event of specific issues end users/consignees should obtain their own legal advice.

22. Will Non-Disclosure Agreements (NDAs) still be required even if a company has BPSS in place?

Yes. A model NDA can be found in the TSP.

23. Will there be legal conflicts if employers have to screen certain employees for substantive contacts with ITAR prohibited nations (for e.g. Syria)?

Dept of State has confirmed that adopting the BPSS will meet the screening requirements. Those UK end users/consignees who decide not to adopt the BPSS will have to introduce their own screening arrangements in order to comply with the rule change.

24. Will employers have to disclose private information to the US Dept of State about employees who are deemed as 'diversion risks'?

If an end user/consignee decides not to use BPSS to meet the screening requirements of the rule change then they may follow the guidance issued by DoS on their website dated 31 August 2011.

25. Will employers need to refuse or remove an employee to work on a project on the basis of a risk of diversion?

The end user/foreign consignee must assess the risk and act reasonably and proportionately in accordance UK law.

26. Currently the use of 124.16 permits the exchange of defence articles with DTCN employees of the approved sub-licensees provided they are nationals of countries that are members of NATO, the European Union, Australia, Japan, New Zealand, and Switzerland, without the need to sign a personal Non-Disclosure Agreement. Where this does not apply or cannot be used 126.18 to provide a mechanism for approval for DTCNs outside of the exempt 124.16 countries. Currently this approval is satisfied using 124.8(5) which must be specifically approved within the MLA/TAA agreement. Subsequently approved individuals are obliged to sign personal NDA's before access to defence articles is permitted. The issue with the current approach, with many European countries, is the conflict with anti-discrimination, human rights and data protection laws when requesting an employee's place of birth or nationality.

The new rule provides additional flexibility which avoids the issues pertaining to the current approach. It is potentially a simpler process provided risks of diversion are accounted for. It provides a choice – end users/foreign consignees could use either approach. Whether adoption of 126.18 clearance or screening procedures in other countries is practical or consistent with their domestic law is a matter for them.

27. Section 124.8(5) will now direct DTCN approvals through 124.16 and 126.18. Does this mean 124.8(5) can no longer be used to approve nationals from countries outside of 124.16?

No. Licensing can still be used pursuant

28. Will existing agreements remain valid but require amendment to incorporate the appropriate 126.18 wording?

DoS have issued updated guidance on this transitional matter through their website.

29. As agreements are amended for other reasons will it be mandatory for the new 124.8(5) clause to be incorporated in place of the old one?

Yes.

30. Can the use of 124.16 and 124.8(5) still be used to approve employees access to defence articles in new agreements or must the provision at 126.18 be used?

DoS have confirmed that end users/consignees have a choice.

31. Who determines if a end user/consignees screening process is robust enough to meet the rule change requirements? Will the TSP only need to be provided at the request of the Dept of State or DDTC or its agents for civil and criminal law enforcement purposes?

If a company uses the standard UK TSP agreed with DoS, there is no requirement in the new rule to have an individual company's security plan endorsed by DoS. Guidance is provided by DoS if a company wishes to pursue or develop its own TSP. The TSP only needs to be provided for civil and criminal law enforcement purposes and DoS understands any disclosure must be in accordance with UK law.

32. Do the screening results need to be provided to the US agreement holder?

No.

33. Is there any requirement for the foreign consignee to maintain records of its sub-licensee DN/TCN approvals?

No.

34. What responsibility does the foreign consignee have towards its sub-licensees?

None. The sub-licensee must ensure that it is compliant with the rule change. The foreign consignee may report its sub-licensees' compliance preferences to the UK exporter.

35. 'Regular Employees' as defined in new 120.39 – that is permanent direct employees plus individuals 'in a long term contractual relationship' with the employer.

(i) Please confirm that sublicensees and contract employees, except those meeting the above criteria are not covered?
(ii) What does "long term" mean?

(i) This is correct.
(ii) Per 120.39, Dept of State has confirmed that a regular employee generally includes individuals working under the direction and control of the company, working full time and exclusively for the company and where the staffing agency has no role in the work the individual performs. This excludes sub-licensees and those working under short term contracts less than a year in length.

36. Can 'temporary staff' be taken to be 'contract employees' as defined in para 3.9b of the DDTC's Agreement Guidelines, i.e. will contract employees with a UK Government BPSS clearance be covered by the 126.18 (c) (2) exemption?

Probably, but HMG is awaiting final guidance from DoS.

37 The provisions of this rule apply explicitly to governments / end users. Is it the intention of government end users to comply with them?

Dept of State understands HM Government will follow the TSP guidance, at its discretion and in accordance with UK law.

38. Do the four key elements of the BPSS fully meet the screening requirements of 126.18 (c) (2)?

Yes – the EoN agreed between the US Government and HMG on 11 August states that the BPSS meets the screening requirements of the rule change.

WorldECR

The journal of export controls and compliance

Contributors in this issue

Jason M. Waite and Diego S. Marquez, Alston & Bird
www.alston.com

Christopher T. Cloutier and Jane Y. Cohen,
King & Spalding
www.kslaw.com

Emilia Stępień and Krzysztof Korwin-Kossakowski,
Bird & Bird LLP
www.twobirds.com

Holger Schmitz, Noerr
www.noerr.com

General enquiries, press releases, subscriptions: info@worldecr.com

Contact the editor, Tom Blass: tnb@worldecr.com tel +44 (0)7930405003

Contact the publisher, Mark Cusick: mark.cusick@worldecr.com tel: +44 (0)7702289830

WorldECR is published by D.C. Houghton Ltd.

ISSN 2046-4797. Refer to this issue as: WorldECR [0107]

Correspondence address: D.C. Houghton Ltd, Suite 17271, Lower Ground Floor, 145-157 St John Street, London EC1V 4PW England

D.C. Houghton Ltd is registered in England and Wales (registered number 7490482)
with its registered office at 145 - 157 St John St, EC1V 4PY, London, UK

ISSUE 7. NOVEMBER 2011
www.WorldECR.com