13 February 2012

AmCham EU position on Industrial Policy for the Security Industry

The American Chamber of Commerce to the EU (AmCham EU) welcomes the efforts by the European Commission towards a Communication on an Industrial Policy for the Security Industry and the reflections that such efforts have generated on how to overcome the hurdles that the European security industry is currently facing.

AmCham EU's membership includes both users and producers of security technologies and services. Following our response to the public consultation in preparation of the Communication, we would like to offer further thoughts on some of the issues that the Commission has identified as possibly requiring action and on the relevant policy areas that could address such issues. In addition, we encourage the Commission to address how services and the single market can be improved in order to support a robust European security market.

Market fragmentation – Relevant policy areas to address the problem

Certification/conformity assessment procedures

AmCham EU supports EU-wide harmonised certification/conformity assessment procedures covering all (or at least as many as technically possible) security products. Currently, national procedures and requirements contribute to trade barriers among Member States. The Commission should consider and promote existing European certification schemes for security-related products and services. Further, we believe that the EU and the US should cooperate more closely in the hopes of a system of mutual recognition of certification and testing standards at the very least, and possibly to the adoption of joint standards. We understand that this cannot happen overnight, but we do believe there should be increased co-operation – both at the political and technical level – on both sides of the Atlantic.

Standardisation

AmCham EU fully agrees that the lack of standards affects the fragmentation of the EU security market. The lack of EU-wide standards for both products and services means that industry must focus considerable attention on compliance with dozens of often-conflicting national requirements, to the detriment of innovation.

We support step-by-step end-user driven standardisation based on a careful evaluation of existing national, European and international standards, via Commission mandates to European standards organisations (ESO).

American Chamber of Commerce to the European Union
Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium
Telephone 32-2-513 68 92 Fax 32-2-513 79 28
Email: info@amchameu.eu

Secretariat Point of Contact: Adriaan Scheiris; adriaan.scheiris@amchameu.eu +32 2 289 10 19

AMCHAM EU
AMERICAN CHAMBER OF COMMERCE TO THE EUROPEAN UNION
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

POSITION STATEMENT

In this regard, we believe it is crucial that standards be truly technology-neutral and based on the desired outcomes and performance of complete systems, rather than the capabilities of individual technologies.

A technology-specific approach to standardisation has the effect of freezing development and deters further investment in alternative technologies, or even in combinations of existing technologies that may offer better performance. Standards should promote development of the best available solutions to address security needs, irrespective of current usage and the product's country of origin.

It is also crucial that timelines for the introduction of new standards are realistic and, once set, are not subsequently changed except in extreme circumstances when no technology is available to meet higher standards. Manufacturers of complex technologies invest over long timeframes according to projections of future market demand and must be able to rely upon the existence of predictable markets if they are to achieve a return on their investment. Postponing the introduction of new standards when technology is available makes future investment less certain and damages the European security industry in the long term.

Fragile industrial base – Relevant policy areas to address the problem

Pre-commercial procurement

Mature markets (such as border surveillance, airport security and critical infrastructure protection) are normally sufficiently large and diverse to attract a level of industrial investment necessary for the development of state-of-the-art products, services and technologies. Emerging security markets (such as automated immigration control, supply chain and cyber security) may need a level of public investment in order to develop and demonstrate world-class solutions. In these latter cases, even limited pre-commercial procurement could encourage European companies to stay the course in product development and deployment while a consolidated market takes shape.

Defence and Security procurement

To reduce the fragmentation via defence and security procurement, the Commission should consider a 'Government Procurement Standard' similar to what the US has with the 'Homeland Security Standard'. By requiring security providers to comply with one set of rules, economies of scale and interoperability can be achieved. Currently, all CCTV and access control products are required to meet many national standards (there are several for cameras, analytics, DVRs, access control software, cabling, networks, intrusion detectors, sirens, etc). Many companies, in particular SMEs, are generally unable to certify products to these various codes, which contribute to a fragmented market and a barrier to expansion beyond one or a few countries.

American Chamber of Commerce to the European Union – Avenue des Arts/Kunstlaan 53, B-1000 Brussels, Belgium
Telephone 32-2-513 68 92 – Fax 32-2-513 79 28 – info@amchameu.eu– www.amchameu.eu

International Markets

It is of vital importance to the development of a vibrant European security industry that the global security market remains open and accessible. Many of the major European players conduct a significant share of their business outside the EU. This diversification helps defray development costs and generates economies of scale for the companies concerned. The EU should, therefore, make full use of its trade policies to maintain and, wherever possible, enhance international market access through mutual openness, recognition and standardisation. For instance, the current EU-India FTA presents a great opportunity to lower or eliminate Indian import duties on security products. The overall industry is suffering from the burden of high taxation that average 25-30% in total. The removal of the basic customs duty of 10% will contribute to levelling the field for European products.

In addition to these policies, bilateral trade and investment agreements should be used and enforced to protect foreign investments and ownership of security services in third countries. There have been proposals to severely limit or prohibit foreign ownership of security providers in various countries. It is imperative that companies can rely on a trade policy that will protect their interests.

Third Party Liability Limitation (TPLL)

Through the deployment of high technology, public/private partnerships and the outsourcing of security-related services, the front-line task of protecting citizens worldwide has increasingly fallen on private sector providers of security technologies and services. These providers, unlike other industries, face the continuous risk of their products and services being undermined by terrorists for political or other purposes. Experience has shown that terrorist incidents can generate unlimited liability exposure which bears no relation to the value of the product or service provided, which is potentially enterprise-threatening for the companies involved, and for which insurance is generally unavailable- a concern shared by providers on both sides of the Atlantic.

Governments have reacted in different ways to assure that the victims of terrorist incidents are appropriately compensated and that industry continues to invest and deploy new technologies to protect against the creation of new victims. Following the 9/11 terrorist attacks, US law allowed companies to limit their liability by having their individual security technologies approved by the Department of Homeland Security (DHS) under the Safety Act.[1] The Act also contains certain insurance requirements that provide compensation for victims with meritorious claims. In France, a fund has been created to compensate

[1] Further information is available at https://www.safetyact.gov/ The SAFETY Act limits the scope and type of damages recoverable by third parties against providers of anti-terrorism technologies (products or services) approved by the Department of Homeland Security, in the event of an act of terrorism. Over 200 anti-terrorism technologies are now covered by the Act. European companies can also submit applications for SAFETY Act approval and protection (for instance, BAE Systems, Siemens and Smiths Detection have availed themselves of such protection).

American Chamber of Commerce to the European Union – Avenue des Arts/Kunstlaan 53, B-1000 Brussels, Belgium
Telephone 32-2-513 68 92 – Fax 32-2-513 79 28 – info@amchameu.eu– www.amchameu.eu

AMCHAM EU
AMERICAN CHAMBER OF COMMERCE TO THE EUROPEAN UNION
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

POSITION STATEMENT

victims of terrorist attacks and thus reduce the burden of risk for technology and service providers. Other schemes exist, although many states within and outside the EU have not as yet addressed the issue. In cases where protection is available, it is generally restricted to incidents occurring within the territory of the nation concerned. A market distortion therefore exists, favouring technology and service providers doing business in those protected markets.

As pointed out in our response to the consultation, AmCham EU believes that the lack of appropriate and consistent TPLL in the EU jeopardises the overall sustainability of the security industry and hampers investment and innovation for the protection of EU citizens with the best anti-terrorism technologies and services. We respectfully suggest that, in order to ensure a level-playing field, to support the development of the best technologies to keep European citizens safe, and to avoid legal uncertainty and costly law suits for determining the applicable jurisdiction, the EU consider the adoption of a Regulation.

In this regard, AmCham EU fully supports the policy proposal that the European industry associations EOS (European Organisation for Security) and ASD (Aerospace and Defence Industries Association of Europe) have developed.[2] This proposed legislative act would acknowledge an obligatory third party liability within the EU for all security technology and service providers up to a defined liability cap. Below such a cap, the security technology or service providers will retain the risk of a potential liability or, alternatively, will transfer it to an insurer (if available) for a premium.

Security Services and its single market potential

Although Member States have their own national security policies and strategies to respond to threats, an EU-wide approach may be better in certain circumstances. Crime and national disasters do not recognise national borders, security services such as alarm receiving centres (which monitors security technology remotely) and disaster response infrastructure should not either. National obstacles such as prohibiting cross-border monitoring or restricting electronic monitoring to only certain businesses contribute to the fragmentation of the security industry.

AmCham EU agrees with the results of the Mutual Evaluation Process of the Services Directive. In particular, key findings such as working to correct misinterpretation and implementation of the Services Directive; undertaking performance checks on specific sectors (in this case, security being a priority); assessments on reserves of activity, capital ownership and legal form; and, enhance transparency to avoid new regulatory barriers will greatly enhance the state of the security industry in Europe.

We applaud the European Parliament for calling on the Commission 'to focus action on the sectors and professions with a high growth potential for the cross-border provision of services'. In this regard, we believe that the Commission should focus on the security sector.

[2] ASD/EOS joint proposal is available at http://www.eoseu.com/LinkClick.aspx?fileticket=jgvkJXP1x9w=&tabid=268&mid=1059

The Services Directive Frequently Asked Questions (FAQs) are clear on what type of security services are under its ambit of application. We agree that such services as '…monitoring of property or persons from a distance through electronic devices are covered'. Unfortunately, these cross-border services are not allowed uniformly across Europe. One early action could be to update the *Handbook on Implementation of the Services Directive* to reflect what is in the FAQs, followed by consultation with the Member States to amend their respective legislation to differentiate between security services that are under the scope of the Services Directive and those that are not.

* * *

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate U.S. investment in Europe totalled €1.4 trillion in 2009 and currently supports more than 4.5 million jobs in Europe.

* * *

American Chamber of Commerce to the European Union – Avenue des Arts/Kunstlaan 53, B-1000 Brussels, Belgium
Telephone 32-2-513 68 92 – Fax 32-2-513 79 28 – info@amchameu.eu– www.amchameu.eu

AMCHAM EU
AMERICAN CHAMBER OF COMMERCE TO THE EUROPEAN UNION
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

POSITION STATEMENT