June 9, 2013

Filed Via Online Submission at www.regulations.gov

Laurie-Ann Agama
Acting Chairman, Trade Policy Staff Committee
Office of the US Trade Representative, Executive Office of the President
600 17th Street, N.W.
Washington, D.C. 20508

RE: Docket Number USTR-2013-0022, Request for Comments on Negotiating Objectives with Respect to Japan's Participation in the Proposed Trans-Pacific Partnership Trade Agreement

Introduction

The Semiconductor Industry Association (SIA) welcomes the opportunity to provide comments on Japan's participation in the proposed Trans-Pacific Partnership Trade Agreement (TPP). SIA is the voice of the U.S. semiconductor industry, one of America's largest export industries and a bellwether of the U.S. economy. SIA unites more than 60 companies from across the United States that account for 85 percent of the nation's semiconductor production.

Semiconductor "chips" are used in everything that is computerized or uses radio waves. Semiconductors are critical components in a staggering variety of products, from smaller computers and smart phones to safer automobiles and navigation systems; from more energy efficient LED lights and appliances to smarter meters and motors; from telecommunications platforms to medical devices. Semiconductors make the world around us smarter, greener, safer, and more efficient and are economically vital to the nation's growth and productivity.

In 2012, U.S. semiconductor companies generated over $146 billion in sales — representing half the worldwide market, and making semiconductors the nation's second largest manufacturing export industry on a five year average from 2008-2012. The U.S. semiconductor industry directly employs nearly a quarter of a million workers in the United States and indirectly accounts for over a million additional jobs in other sectors of the U.S. economy. Economic analyses demonstrate that semiconductors, and the information technologies they enable,

represent three percent of the economy, but drive 25 percent of economic growth. The U.S. semiconductor industry has an especially robust presence in over twenty states and funds research at over 40 U.S. universities.

The United States and Japan have historically been leading trade partners in semiconductors. In 2012, Japan was the 13th leading destination for U.S. semiconductor exports and the 6th leading source of U.S. semiconductor imports. In 2012, total two-way semiconductor trade between the United States and Japan totaled over $3.9 billion with U.S. exports to the Japan accounting for almost $900 million and U.S. imports from Japan accounting for roughly $3 billion. The importance of the Japan market to U.S. companies is much greater since they often design and fabricate products in the United States, export to third countries for assembly and test, and ship to Japan from these third countries. SIA estimates that the U.S. semiconductor industry shipped $13 billion worth of semiconductors to the $41 billion Japan market in 2012.[1] Furthermore, the Japanese and American semiconductor industries have a close working relationship as evidenced by our long standing membership in the World Semiconductor Council (WSC) – a body that furthers cooperation on policy matters related to the worldwide industry.

Given Japan's status as a top semiconductor trading partner, and a valued member of the world trading community, SIA supports the inclusion of Japan in the TPP. SIA encourages the government of the U.S. and Japan to strive for trade and policy solutions that fuel innovation, propel business and drive international competition in order to maintain a thriving global semiconductor industry.

Global Encryption Standards and Regulations

The use of encryption has become more common and widespread in a multitude of commercial ICT applications. Indeed, nearly all ICT products contain encryption to prevent data loss, ensure security and integrity of data (e.g. personal data or in communication) and allow for valuable commercial applications such as mobile payments, e-health, e-passports. However, outdated government security policies remain in place that place unnecessary restrictions on the use of and

[1] World Semiconductor Trade Statistics, 2012

trade in products containing encryption. These restrictions provide too much opportunity that they may be implemented in a discriminatory manner. Moreover, SIA is concerned about various issues, in some regions, related to import and use regulations and licensing & certification requirements and administrative procedures for semiconductors with cryptographic capabilities, including, among others:

- Lack of stakeholders consultation on ongoing reviews of regulations on encryption
- Difficulties in obtaining the needed algorithms and licenses necessary for import, production or sale of commercial products or applications with cryptographic capabilities
- Unjustified difficulties in meeting license requirements
- High administrative burden, unpredictable process and procedures and cost of certification
- Concerns with certifications where only domestic companies can apply to be certified or meet the requirements, or could be favored
- Concerns with encryption standards being turned into technology mandates

Such practices act as non-tariff barriers that significantly impact market access and free trade. Moreover, regulations that directly or indirectly favor specific technologies, limit market access or lead to forced transfer of intellectual property stifle domestic innovation and, in the case of encryption, prevent access to the strongest available security technologies in the market place, resulting in less secure products. Both global collaboration and open markets for commercial encryption technologies should therefore be strongly encouraged as they inherently promote more secure and innovative ICT products.

The WSC, comprised of the semiconductor industry associations in China, Chinese Taipei, EU, Japan, Korea and the U.S., has developed and communicated over the last three years a solid set of encryption best practices and principles to ensure the continued growth of the ICT industry, and the significant demand for and trade in semiconductors. The governments and authorities in each of these regions have subsequently endorsed these principles.

The WSC Principles (attached in Annex 1) generally state that in order to avoid negative impact on the industry's competitiveness, it is important to prevent unnecessary restrictions to trade. As such, commercial products with cryptographic capabilities which are or will be widely available and deployed in the respective domestic markets, should as a general matter not be regulated.

The WSC Encryption Principles strongly encourage the use of global or international standards, including normative algorithms, as essential to avoid fracturing the global digital infrastructure and creating unnecessary obstacles to trade. Because security functions are growing in global ICT products and applications, interoperability has become more critical and thus international security standards such as Common Criteria for Information Technology Security Evaluation will increase in importance.

SIA recommends that the governments of the U.S. and Japan should encourage the worldwide dissemination and use of ICT products with encryption-related capability by incorporating into the TPP the WSC principles on commercial encryption used in widely available ICT as binding commitments and promoting their international adoption.

Regional Stimulus Measures and Provisions of Aid to Failing Companies

While the SIA supports appropriate stimulus measures by governments and authorities, it is the view of SIA and the WSC that government actions should be guided by market principles and should avoid adoption of protectionist or discriminatory measures. The competitiveness of companies and their products, not the interventions of governments and authorities, should be the principal determinant of industrial success and international trade, and assistance should be provided in a market-oriented fashion. This is especially important in times of economic downturn or unexpected economic upheaval.

The SIA recommends that the governments of the U.S. and Japan should commit to measures in the TPP that promote the competitiveness of companies and their products as the key determinant of industrial success and international trade. SIA encourages utilizing the existing Government Authorities Meeting on Semiconductors (GAMS) as a platform to discuss these matters as they relate to the semiconductor industry. SIA believes that the GAMS is an

appropriate venue for participating governments and authorities to discuss and consult on instances of impending provisions of aid to failing companies.

Trade Secret Protection

Trade secrets represent core business assets in the semiconductor industry. Trade secret protection affects the competitiveness of companies, and misappropriation can have a critical detrimental impact on future revenue and profit. Accordingly, strong trade secret protection promotes private investment and innovation, and weak protection has the opposite effect. Inadequate trade secret protection can also inhibit free trade. The WSC notes that the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS) calls on members to provide for the protection of "undisclosed information" that is secret and has commercial value, and to protect such information from disclosure, acquisition or use in a manner contrary to "honest commercial practices."

Theft of trade secrets is a growing problem, and present protection through existing means - unfair competition law, employment law and other branches of law- is often inadequate.

There are difficulties in enforcing trade secrets especially as related to gathering evidence of theft. Unlike other areas of IP, key evidence of misappropriation is not always readily available, and the burden is on the rights holder to produce such evidence, particularly with respect to inevitable disclosure when an employee departs one entity to work for a competitor. There are also difficulties in enforcing trade secrets. Enforcement against the third-party inducer (the hiring entity of a departed employee) is often difficult and remedies against the ex-employee are often inadequate. Also, sanctions are often lenient and thus do not act as a deterrent. The cloud computing environment may make trade secret protection even more unpredictable.

Additionally, many governments are developing an increasing number of overbroad certification systems and other regulatory schemes that require the unnecessary disclosure of trade secrets as a condition of market access. The risk that the required sensitive information will leak to domestic competitors is compounded by the reality that many governments have inadequate safeguards to

protect such information, and some of those same governments desire increased technology transfer from developed to developing markets

SIA recommends that the government of the U.S. and Japan develop comprehensive provisions that implement adequate procedures to protect trade secrets, strengthen trade secret enforcement, and require all TPP Parties to justify the necessity of any disclosures of proprietary information as a condition of market access.

Fighting the Proliferation of Semiconductor Counterfeits

Semiconductor counterfeiting is a global issue which is increasingly affecting all parts of the world. Semiconductors are the "brains" behind an incredibly diverse range of end products and systems with "life, health, safety, and mission critical" applications, such as healthcare and medical equipment, national communication networks, emergency response systems, electric power grids (including nuclear and solar power generation systems), industrial and automation systems, and transportation systems and controls. Given the criticality of these end-use products and systems, the proliferation of counterfeit semiconductor products creates serious risks to public safety and health and to critical infrastructure. In addition to counterfeit semiconductors creating a clear and present danger to the public, counterfeits also result in the loss of intellectual property for the original manufacturer. The sale of counterfeits erodes sales of legitimate products and causes job losses and damage to world economies.

The SIA recommends that the governments of the U.S. and Japan commit to fighting the phenomenon of semiconductor counterfeiting in the context of the TPP, and intensify the implementation of IPR enforcement measures, including domestic, bilateral and multilateral countermeasures and information sharing activities, aimed at combatting the trafficking of counterfeit semiconductors.

Annex 1: WSC Encryption Principles

Lisbon, 23 May 2013

WSC Encryption Principles

Background

The World Semiconductor Council (WSC)[2] recognizes that it is important to ensure that markets will be open and free from any discrimination. The competitiveness of companies and their products should be the principal determinant of industrial success and international trade. Governments and authorities should, therefore, ensure full intellectual property protection, full transparency of government policies and regulations, non-discrimination for foreign products in all markets and removal of unreasonable burdens on world commerce.

Semiconductors are overwhelmingly used as building blocks for computers, mobile phones, handheld devices and many other widely available commercial information and communications technology (ICT) products and systems. The functionality of semiconductors constantly evolves in order to meet consumer demands, which have increasingly called for product features such as encryption that better protect security and privacy in and across a variety of ICT products and systems. The use of encryption thus is not limited to government and military applications but has become widespread, given its ability to help safeguard the integrity and confidentiality of information. As a result, the great majority of applications of encryption involve every day commercial products which are commonly used and traded in the global marketplace.

Indeed, nearly all ICT products contain encryption to prevent data loss, ensure security and integrity of data (e.g. personal data or in communication) and allow for valuable commercial applications such as mobile payments, e-health, e-passports. Although encryption is a secondary feature for widely available ICT products such as garage door openers, mobile phones, ATM machines, internet browsers, DVD players and other common products, consumers demand it in their technological devices to ensure their communications are secure and private. Encryption is now part of the foundation of the internet and e-commerce developments. In many of these applications encryption functionality (besides other functions) is provided by semiconductors.

Regulations that directly or indirectly favor specific technologies, limit market access or lead to forced transfer of intellectual property stifle domestic innovation and, in the case of encryption, prevent access to the strongest available security technologies in the market place, resulting in less secure products. Both global collaboration and open markets for commercial encryption technologies should therefore be strongly encouraged as they inherently promote more secure and innovative ICT products.

[2] The WSC represents global leaders in the manufacturing and design of semiconductors and is comprised of the Semiconductor Industry Associations in China, Chinese Taipei, Europe, Japan, Korea, the United States.

Very few countries have regulations governing the importation and use of encryption. The global trend is toward further de-regulation for mass marketed or widely available IT items in recognition of their widespread use and very limited value in regulating the commercial market.

Encryption Principles

Encryption regulations shall not be used for the purposes of limiting market access for foreign products. To prevent unnecessary restrictions on trade, products with cryptographic capabilities that are, or will be, widely available and deployed -- whether as a result of sales through normal or common retail channels, OEM sales or other means of distribution -- should not be regulated as a general matter except in narrow and justifiable circumstances (e.g., resulting out of international conventions such as export controls to prevent proliferation of munitions and weapons of mass destruction to targeted countries or targeted end users). The WSC Principles make it clear that generally there should be no regulation of cryptographic capabilities in widely available products used in the domestic commercial market because mandating or favoring specific encryption technologies will reduce, not increase, security and also raise product costs.

To the extent that encryption regulation is necessary, the WSC recommends the following practices:

- Regulations should not directly or indirectly favor specific technologies, limit market access or lead to forced transfer of intellectual property to avoid stifling domestic innovation and, in the case of encryption, preventing access to the strongest available security technologies in the market place, resulting in less secure products.
- The WSC opposes technology mandates, including any that involve encryption use in domestic commercial markets, because (i) the significant impact they can have on society and our industry; and (ii) such mandates often become outdated as technologies quickly evolve, and thus they create significant interoperability issues.
- Any regulatory requirements must be applied on a non-discriminatory basis and in a manner no less favorable than that granted to domestic producers (consistent with Articles I and III of GATT 1994), and respect intellectual property rights (consistent with Articles 28 and 31 of TRIPS 1994).
- Global collaboration and open markets for commercial encryption technologies should be strongly encouraged as both inherently promote more secure and innovative ICT products.
- Regulatory procedures related to the notification, evaluation, approval, or licensing of goods containing encryption technology, and the process for exempting goods, should be transparent, predictable and consistent with international norms and practices. They should not impose unreasonable or burdensome requirements on such goods. JSTC shall discuss international norms and practices.

The WSC believes that adhering to these practices will allow innovation and the digital economy to flourish, and ensure that the strongest available security technologies will prevail and be available in all the market places to the benefits of all users of commercial products.

Clarifications

In regard to the use of international standards, norms and practices as required by one of the WSC Encryption Principles, the WSC provides the following clarification and statement:

- Definition of International

  The term international as a word means involvement of, interaction between or encompassing more than one nation, or generally reaching beyond national boundaries. For example, international law, which is applied by more than one country over the world, and international language which is a language spoken by residents of more than one country.

- International Standards

  International standards are standards developed by international standards organizations, which are open to all Members of the World Trade Organization or to most countries of the world. Notable examples of international standards bodies are the International Organization for Standardization (ISO) or the International Electrotechnical Commission (IEC). WSC supports and calls upon government authorities to follow the principles and procedures which have been decided by the WTO Technical Barriers to Trade Committee,[3] when international standards are elaborated by its members.

Examples of security related international standards, norms and practices are:

- Common Criteria (international standard). The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification.

- All testing laboratories must comply with ISO 17025, and certification bodies will normally be approved against either ISO/IEC Guide 65 or BS EN 45011.

- Mutual Recognition Agreement (Plurilateral agreement). As well as the Common Criteria standard, there is also a sub-treaty level Common Criteria MRA (Mutual Recognition Agreement), whereby each party thereto recognizes evaluations against the Common Criteria standard done by other parties. Originally signed in 1998 by Canada, France, Germany, the United Kingdom and the United States, Australia and New Zealand joined 1999, followed by Finland, Greece, Israel, Italy, the Netherlands, Norway and Spain in 2000. The Agreement has since been renamed Common Criteria Recognition Arrangement (CCRA) and membership continues to expand.

The WSC Encryption Principles strongly encourage the use of global or international standards, including normative algorithms, as essential to avoid fracturing the global digital infrastructure and creating unnecessary obstacles to trade. Because security functions are growing in global ICT products and applications, interoperability has become more critical and thus international

[3] Source: Second Triennial Review of the Operation and Implementation of the Agreement on Technical Barriers to Trade, Annex 4, G/TBT/g, WTO Committee on Technical Barriers to Trade (13th November 2000)

security standards such as Common Criteria for Information Technology Security Evaluation will increase in importance.

These security standards often define encryption functions for protection of information and data, as well as specify cryptographic algorithms that are developed or identified for the target application areas. Using standard cryptography as part of common protocols and specifying encryption algorithms to be used (along with making provisions for handling key management, etc.), enables an infrastructure to achieve global interoperability between security functions in products and systems. Whenever possible, the WSC will continue to support greater adoption of international security standards, rather than and instead of technology mandates.

General WSC Recommendations to Governments and Authorities

WSC encourages governments and authorities to advocate for transparency in any additional regulatory developments concerning the use of encryption in domestic commercial markets. Such transparency should include information on proposed testing and conformity assessments related to those regulatory developments. Testing and conformity assessments can create significant market barriers if they are not transparent, non-discriminatory, fully protective of intellectual property rights, based on international standards and done by qualified independent laboratories.

The availability of relevant information gives governments and authorities an option to weigh in on and shape the direction of potential regulatory measures and any implementing rules concerning encryption, which could impact trade in semiconductors and contradict WSC Principles, before those measures and rules are finalized. Indeed, as we noted in the WSC Principles, "The WSC requests the governments and authorities to continue their efforts to ensure that all WTO members observe the principles set forth above." Governments and authorities' efforts to increase transparency and help our industry ensure compliance with the WSC Principles going forward will help keep markets open and allow innovation and the digital economy to flourish.

Endorsement of WSC Encryption Principles by Governments and Authorities

The governments and authorities (GAMS) representing each of the six current WSC regions agreed to encourage all GAMS members and governments in general to observe the Encryption Principles that the WSC has developed since 2009 and to which GAMS members have committed at their annual government and authorities meeting on semiconductors in 2012. The GAMS acknowledged that the WSC Encryption Principles make it clear that in order to avoid negative impact on the industry's competitiveness, it is important to prevent unnecessary restrictions to trade, and that therefore, commercial products with cryptographic capabilities which are, or will be, widely available and deployed in the respective domestic markets should as a general matter not be regulated.

As recommended by the WSC, the GAMS also agreed to helping ensure open global markets that are free from discrimination by encouraging the adoption of international voluntary standards and norms, including algorithms, as essential to avoid fracturing the global digital infrastructure and creating unnecessary obstacles to trade. In the limited circumstances where

regulation may be necessary, the GAMS regions agreed to advocate for transparency and non-discrimination in any regulatory requirements, either in force or being developed concerning encryption in semiconductors used in domestic commercial markets, including the conformity assessment procedures used to demonstrate compliance with those requirements.