

**Global Transshipment and Enforcement Seminar:
Synergies of Strategic Trade Control Elements
Bangkok, Thailand
July 18-21, 2006**

Overview

Co-hosted by the governments of the United States and Thailand, the Global Transshipment and Enforcement Seminar was held on July 18-21, 2006, in Bangkok, Thailand. The conference, as part of the U.S. Department of State's Export Control and Related Border Security Program (EXBS), brought together 159 participants representing 23 countries to discuss the seminar's stated theme—"Synergies of Strategic Trade Control Elements"—as well as recent events, trends and developments in the field as part of ongoing efforts to simultaneously enhance trade security and facilitate free trade.

Mr. John Clark, Deputy Assistant Secretary for Immigration and Customs Enforcement (ICE), Department of Homeland Security, and Dr. Sathit Limpongan, Director General, Royal Thai Customs, delivered the keynote speeches. The U.S. keynote focused on the truly global nature of weapons of mass destruction (WMD) proliferation and the increasingly complex and innovative methods needed to address this threat. The Thai keynote noted the challenge for customs' authorities to balance trade security and facilitation, as well as the positive role played by the World Customs Organization in this regard.

The conference was organized into larger plenary sessions with presentations that appealed to all participants. Presentations in the plenary focused on such issues as: WMD Proliferation Trends and Challenges, the Impact of Export Controls on an Export-Based Economy, and the Global Money Laundering Threat. After this initial plenary session, there were three smaller, more in-depth breakout sessions. They were: Practical Enforcement Techniques, Using Technology and Coordination to Leverage Strategic Trade Controls, and Strategies for Industry Outreach and Compliance. These three breakout sessions gave participants an opportunity to focus on issues in a much more detail-oriented fashion, with an eye towards promoting open and frank discussion, as well as a sharing of experiences among the participants.

A dinner reception hosted by the U.S. delegation provided an opportunity for participants to meet their international counterparts in a more informal environment. On the final day of the seminar, participants were given the option of touring the Port of Bangkok or attending an in-depth demonstration of Tracker, A U.S. Automated Licensing System, and Internal Compliance (ICP) software by officials from the Departments of State and Commerce, respectively.

The Keynote Speeches

In the U.S. keynote speech, Mr. John Clark, Deputy Assistant Secretary for Immigration and Customs Enforcement (ICE) in the Department of Homeland Security, noted that the proliferation of weapons of mass destruction (WMD) is a global threat by nature, and that such global problems require global solutions. Mr. Clark identified the July 2006 missile tests by North Korea as the most recent evidence of the destabilizing role that weapons proliferation can play, both regionally and globally. In response to such threats, it is imperative to close the loopholes in the

global supply chain that nefarious proliferators seek to exploit, Mr. Clark said. A big first step in the that direction was the adoption and subsequent extension of United Nations Security Council Resolution 1540, which established for the first time a binding obligation to enact legal and regulatory measures to effectively implement export controls. Noting that an effective export control system is one that is proactive (i.e. working with industry and the private sector), Mr. Clark stated that Resolution 1540 seeks to build a country's export control capacity from the bottom up, rather than impose it from above. He closed his keynote remarks by acknowledging that while Resolution 1540 has closed key loopholes, others remain and that the greatest threat to global security today is the desire of non-state actors to exploit those gaps to acquire the world's most dangerous weapons.

As the keynote speaker for the Royal Thai government, Dr. Sathit Limpongpan, Director General of the Royal Thai Customs, noted that the key challenge facing customs' agencies is a complex combination of politics and security, in that it is imperative to strike the correct balance between trade security and facilitation. Dr. Limpongpan then articulated some of the current cooperative U.S.-Thai efforts in the areas of port and maritime security, namely the Container Security Initiative. He also noted that Thai Customs and U.S. Customs are currently cooperating on the International Port Security Program, a key objective of which is to help the United States and its global trade partners to improve the security of ports around the world, a program, Dr. Limpongpan noted, that complements CSI very well. Additionally, Director General Limpongpan said that Thai Customs is currently working under the World Customs Organization's Framework of Standards, which set forth the principles and standards necessary to meet the challenges and opportunities of the 21st Century.

The Plenary

Plenary sessions were chaired by Paul van Son, Director of the U.S. Department of State's Office of Export Control Cooperation, in the Bureau of International Security and Nonproliferation.

In the first plenary address, Mr. Sean Kelly of the Arms Control and Counter-Proliferation Branch, International Security Division, in Australia's Department of Foreign Affairs and Trade discussed current trends and challenges in nuclear, chemical, biological, and missile proliferation. Noting that proliferators are becoming more complex in their dealings, Mr. Kelly argued that this threat is not a theoretical one and cited a number of examples to bolster his point. Focusing first on nuclear proliferation, Mr. Kelly noted that generally the nuclear nonproliferation regime has been successfully slowing the spread of relevant technology, but recently it has come under tremendous pressure, citing North Korea's withdrawal and subsequent statement that it possesses nuclear weapons as but one example of the new challenges facing the regime. Moving on to chemical weapons, Mr. Kelly observed that they are relatively easy to manufacture and have been used much more often than other weapons in this category. Noting that many countries have chosen to develop "defensive" biological weapons (BW) research programs, Mr. Kelly stated that this leads to countries possessing a "breakout capability," while increasing the risk of transfer or accidental use of BW agents. Finally, while discussing the current state of missile proliferation, Mr. Kelly noted the important roles that export controls and interdiction have played recently in disrupting such international black markets as the

A.Q. Khan smuggling ring. He closed by saying that while the international image of joint interdiction efforts like the Proliferation Security Initiative (PSI) is often of spectacular at-sea interdictions, most of the hard work of PSI is done in ports by customs officials.

Participants also received a briefing from Patcharadit Sinsawasdi of the Royal Thai Customs on the Integrated Border Inspection Project. Mr. Sinsawasdi noted that this Customs-led project faces the familiar challenge of balancing security with global competitiveness. He pointed out the locations of various Custom Houses on Thailand's border with neighbouring countries and articulated the authorities of officers in their respective areas of responsibilities. He also described the newly introduced 'one stop service center' which includes a Customs House; immigration checkpoint; plant quarantine; FDA checkpoint; animal quarantine station; provincial fish inspection office; and Office of Foreign Trade. Mr. Sinsawasdi noted that while they work to process items for export within one hour and items for import within one day, transshipment items do not fall under the enforcement of national import/export laws and are duty-free.

Two U.S. officials then gave briefings on the current status of two U.S. initiatives—the Container Security Initiative (CSI) as managed by the Department of Homeland Security and the Megaports Initiative as managed by the Department of Energy. Focusing first on CSI, which was announced in January 2002, Mr. Ted Clifton of U.S. Customs and Border Protection in the Department of Homeland Security noted that approximately 25,000 containers enter the United States every day and the major ports that handle much of this cargo are often situated next to large commercial and population centers. The potential vulnerability of the global supply chain necessitates the deterrent role played by CSI, which seeks to discourage the use of containers by terrorists. As the number of CSI participants continues to grow—from 44 currently to approximately 70 by the end of 2007—the need to standardize methodologies becomes even more important, Mr. Clifton noted. In response to the continued threat from terrorism, countries should work to implement some of the following items: smart box technology, integrated container inspection process, remote targeting and webcam inspections, and radio frequency ID tags.

Ms. Elly Melamed from the U.S. National Nuclear Security Administration (NNSA) in the Department of Energy (DOE) then gave an updated on the status of the Megaports Initiative. Explaining that DOE considers the 'first line of defense' to be protecting nuclear materials where they are located, Ms. Melamed stated that the Megaports Initiative was part of the 'second line of defense' that is primarily focused on the detection, identification, and deterrence of, and response to the transfer of nuclear and radiological materials. More than 700 ports ship to the United States, and NNSA has specifically identified 70 ports that it would like to have included in the Megaports Initiative. Anywhere CSI is located, NNSA is working to put Megaports there so inspectors have another tool at their disposal. However, there is a difference between CSI and Megaports, it was pointed out. Unlike CSI, Megaports doesn't station people in ports, as it is a capacity-building program that is equipment focused, while CSI is personnel focused.

Abdul Sani Fauziah from Singapore Customs then gave a presentation on the impact of export controls on an export-based economy, which highlighted the positive

correlation between increased controls and greater volumes of trade. After detailing the legislative basis for Singapore's export control system—namely, the Strategic Goods (Control) Act, and related Strategic Goods (Control) Regulations— Mdm. Fauziah identified the relevant control lists and the penalties for violations of these laws. Noting that Singapore is the busiest port in the world, with some 130,000 vessels passing through annually, the proper balance between security and trade facilitation is vital. But Mdm. Fauziah stated that Singapore's trade volume has increased each of the past three years, just as controls on the transfer of strategic goods have been strengthened. In devising this system, the official said that there were three key challenges: first, how to implement a robust system without negatively affecting trade; secondly, how to overcome limited experience in dealing with controlled items, especially as Singapore is a non-nuclear material producing country and is not a member of any of the four main export control regimes; and third, how to adequately address industry concerns.

The final plenary presentation of day 1 focused on the global money laundering threat, conducted by Mr. Paul Ryan of U.S. Immigration and Customs Enforcement (ICE) within the Department of Homeland Security. He first provided a brief overview of ICE and, more specifically, the Office of Investigations, which focuses on financial crimes, bulk cash smuggling, human trafficking, weapons smuggling, export enforcement, intellectual property rights, cyber crimes, and human rights violations. Mr. Ryan then articulated the three stages of money laundering: placement, which is the disposal of illegal cash; layering, which is the separation of cash from its source; and integration, which is putting the dirty money back into the economy. Of those, placement is the most important and challenging because once the money gets back into circulation, it is very difficult to stop. Now, criminals are increasingly resorting to bulk cash smuggling, mainly as a result of increased enforcement and tightening of anti-money laundering (AML) laws and regulations. Mr. Ryan concluded by saying that ICE works to cooperate with foreign law enforcement counterparts to target criminal organizations involved in bulk cash smuggling, with the seized currency used to support future enforcement efforts.

Breakout Group One: Practical Enforcement Techniques

The participants in Breakout Group One discussed universal challenges encountered while enforcing controls on the transshipment of strategic items. Most presentations focused on the varied policies that the United States government has implemented to meet these challenges, while the discussions that followed the presentations helped identify the particular concerns as well as alternative approaches adopted by the participant countries. The presentations and discussions covered a wide range of enforcement issues, including challenges of communication at seaports and among maritime authorities, the importance of and strategies for providing technical assistance to frontline customs officers, the role of risk targeting in focusing scarce resources, and strategies for coordinating incident response. The group was especially concerned about how best to balance the twin pillars of trade security and trade facilitation as outlined under the World Customs Organization, and welcomed approaches that could support both goals. The participants reached consensus on four important points.

First, they agreed that the global spread of technologies and materials related to WMD production is a shared problem that requires a shared response. Second, this response

must be grounded in strong personal relationships at the local, as well as international, level. Forums such as this workshop were identified as important vehicles for sharing experiences and 'best practices.' Third, through effective communication and tools such as risk targeting, scarce resources can be used most effectively. Finally, the participants recognized that not all responses will work well for all countries, and that solutions must take into account local characteristics.

The first topics that the group discussed were the challenges associated with seaports and coordination among maritime authorities. A presentation from a U.S. Customs and Border Patrol (CBP), U.S. Department of Homeland Security official focused on the difficulties coordinating communication between enforcement officials and authorities at ports. A successful strategy must include shared understanding of business and security goals and communication grounded in personal relationships. When possible, enforcement measures should be designed to take business interests into account. However, all stakeholders must understand that security goals take precedence. Participants raised concerns about how best to balance trade facilitation and trade security, and difficulties expanding the role of customs authorities beyond revenue collection.

A presentation by Mr. Ian Muscat from Malta Customs provided a history and overview of Malta's security efforts at the Port of Freeport. Clear agreements and communication between Malta Customs and Malta Freeport spell out the responsibilities of each agency, while the use of non-intrusive technology such as Vehicle and Cargo Inspection Systems (VACIS) and risk management have minimized delays on legitimate trade. This was followed by a presentation from U.S. Immigration and Customs Enforcement (ICE) examining the special security environment in ports. While ports have regularized schedules and are limited in geographic space, enforcement officials face difficulties carrying out investigations due to the flow of information among port workers. Officials should develop personal relationships with dock employees in order to gain their confidence and support in investigations.

In the conversation that followed, participants asked about specific details of how Malta and the United States receive and vet electronic manifests and the procedures used to investigate and prosecute strategic control cases under U.S. law. Concern was raised about the costs incurred under the 24-hour advance manifest notification rule. A CBP representative responded that the rule had in fact helped keep cargo moving and reduced the tension between trade facilitation and trade security. U.S. presenters also stressed that U.S. policies should be viewed as best practices and may not be practical for all countries.

Two other presentations specifically examined communication between customs and maritime officials. A representative from Argentine Customs provided an overview of Customs' procedures and technologies used at the Port of Buenos Aires. Cooperative and integrative processes are used in order to prevent duplicate processes at the border. The presenter noted that since initiating the Container Security Initiative with the United States, the number of customs interventions at the port had increased. In response, Customs intends to acquire nine more mobile scanners by the end of 2006.

A representative from U.S. Coast Guard outlined initiatives taken since 2001 to improve information sharing. Regional Security Committees bring together industry, port authorities and entities working inside ports to discuss security issues. Local and regional Fusion Centers act as intelligence clearing houses. These information-sharing initiatives have also been valuable combating issues other than terrorism. During the discussion, participants asked about the sharing of intelligence with international partners. Under the third party rule in the United States, the sharing of intelligence information must be approved by the initial agency, though this approval process has improved with the centralization of intelligence agencies under the Department of Homeland Security.

The next presentation from the Australian Department of Foreign Affairs and Trade outlined the legislative base for Australia's export control regime. By the end of 2006, the Australian government is scheduled to complete a review of the 1995 Weapons of Mass Destruction Act in order to ensure a strong coordinated and comprehensive control regime is in place. The presenter noted that Australia uses multilateral efforts such as cooperation in support of UNSCR 1540 as well as regional and bilateral approaches to bolster its strong domestic regime.

Participants asked for details about the extent of export control investigations performed by U.S. Immigration and Customs Enforcement. ICE officials responded that currently ICE has about 5,500 investigators and 56 overseas offices. Generally, these investigators spend between 5 and 10 percent of their time on export control investigations.

Further expounding on this theme, an official from ICE presented details on several case studies to outline the process used to investigate money laundering cases. It was noted that international cooperation is vital for coordinating search warrants and collecting the evidence necessary for successful prosecution. During the discussion following the presentation, participants brought up several other cases of successful international cooperation. One participant mentioned a case where a stored container carrying nuclear power plant components from a dismantled nuclear power plant was successfully blocked from being transhipped. A Thai Customs official explained how a U.S.-funded checkpoint established in northern Thailand to combat drug trafficking had been used successfully to target bulk cash smuggling. Another participant explained the valuable role that the WCO's Regional Intelligence Liaison Offices play in collecting and disseminating information both regionally and worldwide. It was suggested that Memorandums of Understanding (MOUs) with port authorities could be used to promote communication networks.

Another series of presentations explored ways to coordinate the flow of information between front line Customs agents and technical experts. A presentation on the U.S. EXODUS Command Center (ECC) detailed the importance of providing Customs officials a one-stop point of contact for receiving technical information on strategic goods. The ECC maintains liaison officers with the Departments of State, Commerce and Energy in order to provide immediate communication with technical experts. During the discussion that followed, U.S. representatives stressed that setting up a command center need not require a huge outlay of money or manpower, as the U.S. ECC is currently staffed by just five people. A presentation by the U.S. Bureau of Industry and Security (BIS) outlined BIS' role in supporting the ECC.

A representative from U.S. National Nuclear Security Agency presented an overview of efforts to both provide technical reach-back and train Customs officials in commodity identification. While technical experts need to possess both technical knowledge and a thorough understanding of proliferation issues, including export control legislation, front line employees instead need to recognize the red flags that may indicate a controlled strategic good. NNSA currently assists overseas partners in developing trainings for customs officials in commodity identification. In the discussion that followed, participants expressed their concerns that their countries lacked technical resources. It was suggested that countries should work together to create Virtual Technical Experts Centers that could leverage technical skills and expertise regionally rather than just nationally. One representative explained how the customs agency in his country had created a network to connect with university personnel in the faculty of engineering. Participants discussed the limitations of technology and intelligence, and stressed the importance of developing the capabilities of personnel on the frontlines.

Shifting the discussion to risk targeting systems, a Customs and Border Protection official outlined the U.S. approach to targeting containers for inspection and provided information on the Container Security Initiative (CSI) with special attention to its implementation at the Port of Laem Chabang in Thailand. CSI was described as part of a layered response to push back U.S. borders and facilitate the movement of containers at U.S. ports by pre-screening at foreign ports. The methodologies and risk management principles used to identify high-risk shipments help to focus limited resources. The advantages of using an automated customs system were articulated by a presentation from a U.S. CBP representative. Using automated systems such as the U.S. Automated Commercial Environment, information from a variety of sources (including importers and carriers, as well as law enforcement) can be analyzed in real-time. This allows for enhanced screening and tracking of shipments, and provides benefits to businesses through improved logistics management.

The participants were especially interested in how the United States and Thailand cooperated under the CSI program. It was explained that under the program, the U.S. inspectors are guests and do not have the authority to open containers, so they must request assistance from their Thai counterparts to perform non-intrusive or physical examinations of high-risk containers. Furthermore, non-intrusive inspections are performed on about 20 containers per week, and only two containers had been physically opened in the last nine months. Since the lag time at U.S. domestic ports is significantly longer than that at foreign ports, businesses accrue a clear advantage through pre-screenings at foreign ports under CSI. One participant expressed concern about his countries' lack of experience in targeting, while another participant mentioned that his country was still doing targeting manually and had yet to develop an electronic targeting system. U.S. representatives stressed that having the targeting principles in place was more important than the technologies used to carry out targeting.

The final issue discussed involved coordinating incident response. A U.S. Coast Guard representative articulated the expanded role Coast Guard has assumed in security since 2001. Previously, the Coast Guard spent 10 percent of its time on security issues, such as interdicting drug shipments, while 90 percent was spent on

other issues including maritime safety. Now, the Coast Guard devotes 40 percent of its time to securing U.S. waterways. He noted that the Coast Guard has been able to adapt many skills from search and rescue to performing tactical security measures. One problem noted was that response teams from the Coast Guard, Navy and FBI are unable to intermix, as the teams do not cross-train. The second CBP presentation detailed Customs officers' role in incident response. It was explained that Customs officers are trained to act as first responders, and when they encounter a hazard, they are responsible for establishing control of the perimeter, isolating the hazard and notifying authorities in order to call in specialist support teams. Finally, a representative from Australian Customs provided observations from examining the history of past incidents. She concluded that two areas in particular still need work: coordination among agencies and countries, and strategies for communicating with the public.

Breakout Group Two: Using Technology and Coordination to Leverage Strategic Trade Controls

In this breakout session, much of the discussion revolved around a number of key principles for strengthening domestic capabilities in controlling transshipments. These principles included the understandings that: risk management techniques are important for mitigating dangers and optimizing limited resources; interagency coordination is vital for effective enforcement of transshipment and other strategic trade controls; harmonization of strategic trade controls will serve to strengthen supply chain security; and government-industry partnerships are critical in ensuring compliance and supply chain security.

An overarching theme that also came out of the presentations and discussions in this breakout group was that the complexities involved in controlling transshipments in particular, and other strategic trade in general, have made utilization of technology an essential tool for increasing efficiencies. At the same time, the group also generally agreed that technology could not fully replace well-trained and knowledgeable personnel in making determinations about suspect shipments or transactions. Another important theme that was highlighted during multiple presentations was the importance of reaching out to industry, bearing in mind the vast majority of the global supply chain is in the hands of the private sector, such as exporters, brokers, and shippers.

The group's discussion on coordination began with an overview of the World Customs Organization's Framework of Standards (WCO Framework). This agreement—adopted in June—represented key priorities for the international customs community and was designed to strengthen supply chain security while facilitating legitimate trade. The group discussed the aims of the WCO Framework, which included the harmonization of electronic advance cargo information requirements; promotion of common risk management approaches; establishment of a system of customs inspection in departure countries; and creation of incentives for the private sector to facilitate customs-business cooperation on supply chain security. The WCO Framework aims to get countries to move in tandem in order to avoid distortions in the global supply chain that could create loopholes for illicit trafficking to exploit.

During the discussions on the WCO Framework, participants highlighted the problem of uneven implementation, noting that many countries still lack sufficient capabilities

to fulfil the aims of the framework domestically. A concern was expressed by some participants that the voluntary nature of the framework and the open-ended timeline of implementation would water down the effectiveness of the agreement. While this concern was considered valid, it was noted that forcing a timeline for implementation of the framework would not be feasible and would likely result in the creation of many unsustainable systems. In order to attain global supply chain security, many countries will require monetary and expert assistance from WCO and donor countries to fully abide by the framework's principles. The issue of coordination of international activities related to supply chain security was also identified as an issue that required attention in order to avoid different agencies and organizations enacting contradictory or overlapping regimes that would create an undue overburden on the supply chain.

In keeping with the stated theme of the breakout group, participants held active discussions on the development of technologies that could assist with the management of supply chain security. One such technology that received the group's attention was that of "smart containers." Current research into smart containers is exploring technologies that will enhance capabilities for tracking the movement and handling of containers. This could include, among other things, registering if a container has been opened during transit. The eventual use of this type of technology was described as a force multiplier in a layered approach to supply chain security. A number of technologies were discussed in the breakout group session, although most were still in the research and development phase. It was generally understood that no matter which technologies are ultimately developed in this field, it is essential that all relevant international actors coordinate efforts so that a global standard could be followed.

Participants of the breakout group also explored the issue of targeting and risk management techniques to allow for more informed decision-making about the necessity of intervening and inspecting any given shipment. Attention was given to the importance of interagency coordination for effective targeting and making risk assessments based on a number of different sources, including the profiling of entities involved in the shipment, relevant intelligence data, and detailed knowledge of the commodities involved. Use of technology, such as advanced IT systems and non-intrusive inspections (NII) equipment, can leverage the ability of governments to effectively target suspect cargoes and thereby mitigate risks of illicit transfers occurring.

Within the discussion of targeting and risk management, U.S. participants explained the layered approach taken by the United States, which includes initiatives like the Container Security Initiative (CSI), the Customs-Trade Partnership Against Terrorism (C-TPAT), the Fair and Secure Trade (FAST) program, and Megaports. U.S. representatives additionally focused on the important work of the automated targeting units at ports and the U.S. National Targeting Center. While many systems use automated technologies for targeting, it was stressed by a number of participants that a system could remain paper-based, so long as it was capable of analyzing large amounts of information. Having trained and knowledgeable agents was recognized as an essential part of a risk management system, as it was ultimately up to personnel to judge the significance of anomalies in the supply chain and determine relevant risk factors.

The issue of targeting transshipments was recognized by many in the group as being particularly challenging as it involved a significant paradigm change for customs authorities. As transshipments do not typically interact with the domestic market, customs and licensing authorities in most countries have paid little attention to transshipments in the past and focused mainly on imports and exports. As a result, many countries have limited regulations for controlling transshipments. Transshipment was characterized by one speaker as the “weak link” in the global supply chain since the information about containers transiting through a port has until recently been minimal, while authorities in the transit port have limited time to investigate any anomalies—normally just a few hours. Group discussion placed emphasis on the need to gain as much knowledge about transshipments as possible prior to arrival in the transit port.

During the discussion of transshipment targeting, the principle of coordination, both domestically and internationally, was again highlighted as essential. The ability to determine if intervention is necessary depends on communicating with other relevant parties, especially with the authorities in the country of origin and the private sector entities involved. Tying transshipment controls to the larger picture of strategic trade controls, it was also noted during the group’s discussion that effective export controls in the origin country could ultimately diminish the need for transshipment controls as the necessary interventions would occur earlier in the process and the transit country would feel more secure that high risk shipments would have been stopped prior to export from the originating state.

Another key issue discussed in this breakout session, and one seen as essential to the effectiveness of controlling transshipments was the establishment of linkages between line officers and technical experts. As part of this discussion, participants were given a series of presentations on relevant aspects of the U.S. system, such as the EXODUS Command Center and the use of experts from U.S. national laboratories to advise customs and licensing officers. It was noted that each country should work within their own local conditions to establish an effective means for involving technical experts in the strategic trade control process. One case discussed was that of Malta, where the customs and licensing authorities have begun a partnership with local academic institutions to create a network of experts to advise on commodity export and transshipment-related issues. This concept of identifying domestic expertise was also evident in response to concerns that were raised over the inability of some national custom authorities to safely handle risky or suspect shipments, such as dangerous chemicals or radiological substances. To address this issue, it was stressed that customs agents should coordinate regularly with other relevant domestic agencies so that line officers know whom to call on for domestic expertise when such incidents occur.

Challenges faced by line officers, such as customs agents, were the focus of discussion on coordination of incident response during this breakout group. The importance of interagency response was highlighted as necessary for successful response to incidents that may occur during transshipment interdictions, or for any other emergency situation that may occur at a port or in the open sea. Knowledge about the distribution of responsibilities throughout the varying agencies involved is vital to assuring that a response is effective. It was stressed during presentations in this breakout session that authorities need to have in place preset plans that effectively

bring relevant expertise together in order to assure an appropriate response. Communication between different ports of entry and different relevant agencies could go far in preventing or mitigating a dangerous incident, allowing line officials to be on the look out for suspicious events or activities. Since the potential damage of a chemical, biological, radiological or nuclear (CBRN) attack is high, preparation for such an attack is vital. Once an incident occurs everything should come into place.

It was noted in a number of sessions of this breakout group that the private sector also shared responsibility with government for maintaining supply chain security. The final session of the group further reiterated the importance of reaching out to industry and how these efforts could improve the enforcement of transshipment controls. A number of presenters discussed methods being used by their respective countries to reach out to domestic industry. With the private sector so heavily entrenched in the supply chain, the voluntary compliance of business is essential to assuring container security. Creating incentives for companies to be active partners with government in securing the supply chain is essential for creating an efficient system. As was noted by one speaker, the prevention of strategic trade control violations—via outreach and education—is much more cost effective than enforcement through prosecution.

Breakout Group Three: Strategies for Industry Outreach and Compliance

The participants in Breakout Group Three focused on the many challenges of and strategies for undertaking industry outreach efforts. Recognizing that industry self-policing is the first line of defense in preventing proliferation, breakout participants discussed many of the different models used for effectively engaging and training the private sector to increase compliance with strategic trade controls. Covering a wide range of industry-related topics, presentations were given on the current outreach efforts of the United States, Australia, Japan, Singapore, and South Korea. Additionally, participants heard presentations on supply chain security, industry concerns, challenges between private port authorities and enforcement officials, and the benefits of internal compliance programs and national registration, as well as a demonstration of U.S. Tracker- Automated Licensing System.

Participants expressed particular interest in how to best engage industry and increase private sector awareness while not hindering free trade or expending substantial resources. There were several other key points upon which the participants of Breakout Group Three agreed. The first was an affirmation of the truism that governments cannot monitor 100% of exports, which means that they must rely on industry to self-monitor itself through increased awareness and internal compliance programs (ICPs). Secondly, it was agreed that export control authorities can be effective when trade and industry are involved in formulating rules and regulations, and that viewing industry as a valuable partner and informing them of the national security aspect of trade controls helps this process run smoothly and reduces inadvertent transfer of controlled commodities. Thirdly, based on the fact that statistically the majority of export control violations in the United States, Japan, and Korea are unintentional, there is a strong need for increased industry outreach efforts, raised awareness, and training to industries, especially for small- and medium-sized businesses.

The fourth point that found agreement in the group was that there is a positive correlation between enhanced trade security (export controls) and trade facilitation, as

evidenced by Singapore reporting that its trade has steadily increased while enacting increasingly stringent trade controls. It was also noted that information from industry (employees, competitors) is a valuable source of information on export control compliance and possible violations. Additionally, it was agreed that there are many different ways to conduct industry outreach: seminars, one-on-one consultations (phone calls, emails, company-specific site visits), publications (online, brochures, annual reports, pamphlets, newsletters), conferences, etc., and that these efforts can be adapted to fit a country's available resources while fulfilling the necessary outreach goal.

There was also agreement on a number of points relating to developing capabilities to increase the efficacy of industry outreach efforts. The first of these was that developments in information technology (IT) like websites and email notices are effective ways to reduce demand on small government offices and business resources and can help utilize scarce resources more effectively. Similarly, it was noted that developing and using automated application or license processing systems (e.g. Tracker, TradeNet, Strategic Export Control System) can help expedite processing. Secondly, participants agreed that having a single point of contact to gather and disseminate information from government agencies (like the Exodus Command Center in the U.S.) can provide a vital link between border/port and licensing officials. It was noted that the U.S. experience points to the fact that this point of contact need not be labor or financially burdensome, as only five officers currently work in the EXODUS Command Center. Thirdly, the increasing use by some countries of quasi-governmental organizations (like CISTEC in Japan, STIC in Korea) can aid government ministries in staying current on export control revisions to regime control lists, as well as helping to develop toolsets for industry and enforcement for use in strategic trade control. Additionally, it was noted that because countries often have many agencies involved in the export control/licensing process, inter-agency coordination through working groups and linked information sharing systems has proven to be useful in expediting the process and building consensus. Finally, it was agreed that the creation of an end-use/end-user review capability is vital to effective licensing and enforcement, while pointing out that many foreign-compiled lists of end-users of concern are readily available on-line.

The first set of presentations given to the participants of Breakout Group Three focused on the current outreach efforts of various countries, starting first with the United States. This briefing began with a brief explanation of the U.S. Export and Border Related Security (EXBS) Program, which is the main initiative of the United States government to implement its obligations under U.N. Resolution 1540. The EXBS Program has worked in 57 countries to date, including Malaysia, the Philippines, Singapore, Thailand, Vietnam, Kenya, Mexico, and Jordan, in addition to doing software and compliance training to industry in Russia, Ukraine and Turkey.

The U.S. official then articulated the five pillars to an effective export control system: 1. Developing the legal and regulatory framework, not only for exports, but also for transshipment and transits; 2. Possessing an effective licensing system, which has to be an inter-agency process; 3. Having adequate enforcement capabilities, where officers know the laws they are enforcing; 4. Robust industry outreach and public relations, as industry is the first line of defense; and 5. Interagency coordination, as the enforcement people need to talk to the licensing people.

An official from the Department of Foreign Affairs and Trade (DFAT) then explained some of Australia's industry outreach mechanisms. While Australia conducts some of its outreach activities through its role as the permanent chair of the Australia Group and as this year's chair of the Wassenaar Arrangement, it also engages in scoping visits to clarify current procedures and identify gaps in foreign countries. An active partner in the Proliferation Security Initiative and host of the PSI Pacific Protector 06 exercise, Canberra also conducts PSI-related outreach activities as it seeks to draw more of its Asia-Pacific neighbors into the Initiative. Finally, the official identified the three principles upon which Australia's approach to counter-proliferation is based: First, it is tailored to meet needs of host country, following consultation; Second, it focuses on areas of Australian expertise; and three, the goal is to compliment other work in the field rather than duplicating it.

An official from Japan's Ministry of Foreign Affairs then gave a briefing on Japan's industry outreach efforts, highlighting the very prominent part it plays in the overall Japanese export control model. The emphasis is on internal compliance programs (ICP) and company self-monitoring, he noted, stating how important it is to treat industry as a valuable partner in this process, and the need to engage industry at the management level. Raising awareness is another key element of Japan's export control system and not just with industry but also among government officials, too. The various export control training workshops and seminars were also detailed, with an emphasis placed on explaining the role of the quasi-governmental Center for Information on Security Trade Control (CISTEC), which includes both industry representatives and government officials (semi-retired) that serve as intermediaries between the government and industry.

A presentation from a representative of Singapore Customs then provided a briefing on how Singapore approaches the issue of industry outreach. The official first identified some of the mediums used by the Singapore government in this endeavour, such as news releases, training courses, seminars, mailing lists, field visits, task forces, and circulators. In addition, an updated strategic goods control website has also been launched (www.stgc.gov.sg) where permits and application forms can be downloaded and exports can find out if their products for export products fall under related control lists. The website is also used to post, when necessary, new releases and circulars, while companies can also add themselves to mailing lists to receive updated information relating to strategic trade controls. Finally, it was noted that in 2006, a customs-industry partnership was formed to build industry confidence in government actions and to encourage compliance and acceptance of any new measures imposed.

Another series of presentations focused on industry concerns and how best to effectively address them. An official from South Korea's Ministry of Construction, Industry and Energy (MOCIE) detailed the legislative basis for his country's export control system, and identified which ministry had authority over which type of export. For example, dual-use items are handled by MOCIE, while munitions are dealt with by the Defense Acquisition Program Administration, nuclear items are handled by the Ministry of Science and Technology, and any item being exported to North Korea falls under the jurisdiction of the Ministry of Unification. From seminars, surveys, and visits, MOCIE has found that the biggest concerns are that it is hard to recognize

the ultimate end user; lack of expertise in dealing with strategic items, don't know the latest export control rules; the additional cost for implementation of regulations; that it is complex and inconvenient to get a license; and that it is difficult to understand U.S. regulations, such as the Export Administration Regulations (EAR). To address these concerns, MOCIE has begun to send out email notices, as well as run magazine advertisements and do road shows and presentations in industrial complexes. It has also launched a strategic trade control website that has reduced the need to visit government and public offices, and shortened by 4 days the examination period for export licenses.

In the ensuing discussion, it was noted that officials at the border or port should never make licensing determinations, as that should be the sole job of the licensing authority. Additionally, there was a lot of discussion regarding the link between the harmonized customs codes and the control list numbers, and it was noted that this link is not, and might never be, 100%. It is therefore important to view control lists and information databases as a reference tool rather than an instrument for making licensing determinations.

Using the deemed exports rule in the U.S. as a case study, an official from the U.S. Department of Commerce gave a presentation on how to include industry input in formulating government regulations. The official gave a brief history of the deemed export rule, which deals with foreign workers illegally acquiring U.S. technology for transfer to their home country. There was a desire to actively include the business community and other parts of the private sector, so the Department of Commerce posted a lot of info on its website, and conducted over 120 training programs for universities, government research institutes and laboratories, and the business community. In the end, decided not to publish any rule at all, though through this process, the Department of Commerce hopes to get more effective rules, more knowledgeable audience, and improved compliance.

The next series of presentations focused on the challenges between private port authorities and enforcement officials. The first briefing noted that from the government standpoint, it is vital to develop a strong relationship with private terminal managers and for each side to understand their counterpart's mission. It was pointed out that while technology can sometimes facilitate communication between the two sides, technology is not a cure-all, and that more ground-level efforts like focus groups can promote transparency and ease communication problems.

There was also a briefing on the evolution of the Maltese port of Freeport, and the ongoing relationship between Maltese Customs officials and the private port authorities. It was again noted that the primary challenge is the balance the two pillars of free trade and trade security. To that end, Malta is working with the United States to utilize the best technology available, such as VACIS, which has proved to be a very effective tool because it eliminates the need to physically inspect many containers, thus expediting the movement of legitimate goods.

To help facilitate cooperation between government officials and private port authorities, in 1981 the United States established the Exodus Command Center (ECC) to serve as a 'one-stop shop' for information relating to a suspicious person or cargo at a port or border. The U.S. official conducting the briefing explained that the ECC

will conduct research on the commodity and determine the status of the good, through coordination with all relevant agencies, such as the Departments of State, Commerce, Defense, Treasury, Energy, and the Drug Enforcement Agency (DEA).

Another series of presentations focused on industry compliance itself, with presentations from three countries all describing their understanding of industry compliance within their country. First, a South Korean official stated that private sector surveys found that while there was a high level of awareness of strategic trade controls—as high as 88 percent—the level of implementation was much lower, only around 20 percent. To combat this trend, ICPs were started in a number of large companies starting in 2005. Now, the government is working to support small and medium-sized business with minimal resources increase their traditionally low implementation rates. One way to do this, it was pointed out, is by developing strategic trade software tools, which can minimize the amount of manpower needed, while increasing efficiency through one-stop service.

A presentation from a Japanese official noted that 88% of the illegal exports in Japan are unintentional. Of those, the majority are due to the insufficient nature of the export control system (35%), misjudgement of applicable articles (30%), mistakes in confirmation of shipment (8%), and non-compliance with licensing conditions (15%). The Japanese Ministry of Economy, Trade and Industry (METI) encourages exporters to develop ICPs, submit the ICP to METI for review, and to submit an annual report examining export control implementation. The official identified the basic elements of an ICP- record keeping for at least 5 years, reporting, guidance for subsidiaries, audits, shipping confirmation, organization, and employee training.

A U.S. official echoed the point made by the Japanese official that many of the export control violations that take place are unintentional. Therefore, the U.S. government places a lot of emphasis on training, often with multi-agency expertise. Specific to the Department of Commerce, they conduct both one and two-day programs for exporters that are audience-specific. There are also specialized programs, such as update conferences, technology encryption, export management systems, and how to classify an item (under what control number the product falls). In the discussion that followed, it was noted that voluntary disclosures from the business community form the vast majority of leads in export control violation cases, especially since identifying themselves can serve as a mitigating factor in penalties/punishment.

The final presentation of day two focused on the World Customs Organization's Framework of Standards, the main role of which is to establish standards that provide supply chain security and facilitation to promote certainty and predictability in trade. The presenter noted their four key elements: harmonized advanced electronic cargo information; a risk management approach to address security threats; customs inspections that can be done on behalf of customs administrations if a suspicious transfer is noticed; and benefits for businesses that meet minimal supply chain security standards. Noting that any shutdown in global trade would have a devastating effect on the global economy, the presenter stated that the customs-to-business pillar of the Framework of Standards must be based on dual concepts of equal partnership and shared interest in securing the global supply chain.

Another topic discussed in Breakout Group Three was incident response coordination. The first presenter, from the U.S. Coast Guard, noted the changing role that the Coast Guard has played since the September 11, 2001 terrorist attacks. Before Sept. 11, 90 percent of the Coast Guard's job was search and rescue, while 10 percent was for security (and most of that was domestic). Since Sept. 11, 40 percent of all Coast Guard assets and money go to homeland defense. Also, since those attacks, the need to train for non-standard boarding—boarding a vessel at sea using non-traditional methods—has increased. An Australian official noted that the key aspect of incident response is the need to plan a response to an event before it actually happens. Communication and coordination are key issues and potential stumbling blocks to an effective incident response plan, but each time a response is practiced, the effectiveness and efficiency of that response increases.

Focusing on the role of Internal Compliance Programs (ICPs), a briefing from a U.S. Department of Commerce official noted the strong positive correlation between economic growth and effective export control systems. Beyond that, four key benefits of an effective export control system were identified: to prevent the spread of WMD; to further foreign policy objectives; to honor international obligations; and to protect limited resources when depleting such resources might have longer term foreign policy implications. Within the United States export control system, it was noted that industry has a number of channels for input- from requests for public comments to technical advisory committees, from the President's Export Council to public forums.

The final presentation in Breakout Group Three was a demonstration of the U.S. Tracker program, an automated licensing system. The U.S official pointed out that Tracker's primary goal is to increase the effectiveness of licensing procedures and practices by providing a single channel of communication between technical experts, intelligence agencies, foreign policy officials, and licensing officers which ensure transparency and encourages inter-agency cooperation. Tracker is currently available in 13 foreign languages and provides support to enforcement officials. For example, for customs officers, if a shipment is stopped at a port with questions about the license, the officials can access Tracker to resolve any questions regarding that license; or if there is a question about a particular dual-use item, the official can take a photo of the item, upload the photo and send out to other ministries or agencies for their technical input.