Remarks by David W. Mills

Assistant Secretary, Export Enforcement

Bureau of Industry and Security

Washington, DC July 24, 2013

Good morning, and welcome to Day Two of Update Conference 2013. I'm joined today by five of my colleagues, each of whom plays a crucial role in Export Enforcement at the Bureau of Industry and Security. After my remarks, they will participate in an Enforcement panel and can answer any of the questions you may have.

This is my fourth year as the Assistant Secretary for Export Enforcement. Today, we are on the precipice of achieving the most significant accomplishment to date in Export Control Reform. For the first time in a generation, we're taking significant and concrete steps to make our export control system more efficient and transparent for exporters. Just as critically, we're creating more effective safeguards – what we call "higher fences" - to keep U.S. commodities and technology away from foreign entities who seek to harm our national interests.

What I'd like to talk with you about today is how Export Control Reform is changing and enhancing our enforcement efforts. I'm also going to update you on new authorities Congress granted the Government last year to go after a new category of exports to Iran. And finally, I want to talk about some recent enforcement cases that illustrate how we are bringing our resources to bear to address the threats that violations of export controls pose for our national security and foreign policy.

Before I elaborate on these recent developments, let me say a word about the organization I lead. This past year marked the 30th anniversary of the establishment of a criminal law enforcement capability – the Office of Export Enforcement (OEE) - within what is now known as the Bureau of Industry and Security, or BIS, at the Department of Commerce. Over the past 30 years, Export Enforcement at BIS has evolved into a sophisticated law enforcement agency, with criminal investigators and enforcement analysts who are singularly focused on export control, working closely together with licensing officers within a single bureau of the government. This Administration has made a special point of encouraging more American businesses to export overseas, while maintaining our security and foreign policy objectives. That is why the role of Export Enforcement

within the Commerce Department has been described as “playing defense” on the export promotion team, an apt characterization. Using our subject matter expertise in the area of export controls, coupled with our unique and complementary administrative enforcement tools, we have also leveraged relationships with other federal agencies and with our partners in industry to maximize the impact we are having.

BIS maintains Special Agents at offices in nine cities across the United States. We also have agents co-located with the Federal Bureau of Investigation in Cincinnati, Ohio, Minneapolis, Minnesota, Portland, Oregon and Phoenix, Arizona. In addition, BIS has Special Agents assigned with the Department of Commerce’s Foreign Commercial Service to conduct end-use checks to safeguard the disposition of U.S.-origin items exported abroad. These Export Control Officers (ECOs) are assigned to six strategic locations that are critical to our mission: Beijing, China; Abu Dhabi, the United Arab Emirates (UAE); New Delhi, India; Moscow, Russia; Singapore; and Hong Kong. Some of these ECO positions have regional responsibilities that extend their reach to an additional twenty nine countries.

Our ECOs play a unique and critical role in the fight against proliferation and illicit diversion by spearheading our end-use check program. Last year, end-use checks conducted by our ECOs, supplemented by Sentinel trips by our domestically-based agents, reached a five-year high of almost 1,000 checks conducted in more than 50 countries. In addition, our ECOs have helped us establish robust enforcement-led relationships with the governments of our key transshipment partners in the UAE, Hong Kong, Malaysia and Singapore.

As the Under Secretary stated yesterday, a key priority of our enforcement effort is evaluating the reliability of recipients of U.S.-origin items. To augment our end-use check program, the Office of Enforcement Analysis (OEA) within Export Enforcement is working with the Department of State to coordinate end-use checks where U.S. Munitions List (USML) and Commerce Control List (CCL) items are co-located, so that both organizations can expand the number of overall end-use checks conducted by the U.S. Government. Just last month, we initiated this effort with great success. Exporters should expect that documentation requests

to support end-use checks for both USML and CCL items will become routine beginning in October.

When a foreign party is determined to be an unreliable recipient of U.S.-origin commodities and technology through end-use monitoring, OEA takes a variety of actions, such as screening future license applications involving that party, referring a lead for further investigation by OEE Special Agents, or taking an administrative action, including Entity List or Unverified List designation.

A key part of this effort is providing information to exporters about suspicious procurement activities and actors. For example, over the past 18 months, OEA has ramped-up our Guardian Lead program whereby Special Agents have reached-out to more than 120 companies about suspicious requests for procurement. This program creates a critical communication link between U.S. companies and Export Enforcement at BIS, allowing unwitting U.S. suppliers to avoid filling orders to nefarious actors and providing the U.S. Government with valuable information about illicit supply chains, including the ability to impede their procurement efforts.

Through front companies, terrorists and rogue regimes are sourcing innocuous electronics and explosive material that might lead to tremendous harm to our service men and women. Don't be an unwitting supplier to these illicit schemes. You should apply additional vigilance to requests for exports of items to transshipment countries, whether or not requiring a license, and particularly if an end user is not identified. The majority of our unfavorable end-use checks take place in transshipment destinations. Therefore it is critical that you adequately screen your customers in these locations.

Finally, no picture is complete without reference to the Office of Antiboycott Compliance (OAC). This year the OAC celebrates its 35th year of operation and continues to actively pursue its compliance mission. OAC carries out its mandate through a threefold approach: monitoring boycott requests received by U.S. businesses, bringing enforcement actions when necessary, and guiding U.S. businesses on the application of the Export Administration Regulations to particular transactions. In addition to these traditional compliance tools, OAC goes to the source to eliminate boycott requests at their origin. By working with its government partners in the Office of the U.S. Trade Representative and at the Department of State, OAC has met with the ministries of boycotting countries

issuing the most boycott-related requests. By meeting with these governments and pointing out the barrier to trade that boycott requests impose, OAC often is able to remove prohibited language, enabling U.S. businesses to compete on an equal footing in this region of the world.

Over the last year, OAC officials conducted two antiboycott compliance assessment trips to the Mideast. These trips are designed to assess boycott compliance in boycotting countries and to provide in-country training and support to U.S. embassy and U.S. Foreign Commercial Service officials on the antiboycott regulations. OAC officials were able to establish a bilateral arrangement with the UAE – our largest trading partner in the Mideast – so OAC is able to utilize the auspices of the UAE's Commercial Attaché in Washington to resolve boycott-specific problems. It's a positive first step and we appreciate their cooperation.

In March of this year, a senior OAC official travelled to Baghdad to participate in the first meeting of the trade and investment subgroup of the U.S.-Iraq Joint Coordinating Committee (JCC). The JCC trade and investment subgroup focused on nontariff barriers to trade. U.S. companies have encountered a significant

number of boycott-related requests contained in commercial documents over the last decade. Nearly all of the prohibited requests from Iraq reported to OAC in 2012 were either tender documents from the Iraqi Ministry of Health or a boycott questionnaire given to U.S. companies from the Iraqi Patent Office. The U.S. committee members proposed an approach to eliminate boycott language that will involve future technical assistance from OAC.

Export Control Reform: Regulatory Developments

As you heard yesterday, the Administration has made significant progress over the past year to implement the President's Export Control Reform initiative. And we are three months from initiating the transfer of aircraft-related items from the International Traffic in Arms Regulations (ITAR) to the Export Administration Regulations (EAR) to facilitate interoperability with our allies and partners, help make our defense industrial base more competitive, and allow the government to concentrate its resources on what really matters. This is the first implementation step in the transfer of literally tens of thousands of munitions and satellite-related items to the EAR over the coming year. Although the majority of the focus has been on the transfer of items from the USML to the more flexible licensing regime

of the CCL, the effort to erect higher fences around these control list changes has been every bit as important.

Export Enforcement at BIS will carry out its responsibilities to ensure that the regulatory changes implemented under the President's Export Control Reform initiative are properly monitored and enforced. We have been sitting side-by-side with our regulatory and policy counterparts in Export Administration at BIS as this process unfolds, providing key insights from three decades worth of investigations. Certain regulatory changes are of particular benefit to our enforcement efforts.

The first – License Exception Strategic Trade Authorization – or STA, will authorize the export of munitions items moved from the USML to the newly established "600 series" in the CCL to 36 allied and partner nations for ultimate end use by the governments of those countries. Under STA for munitions items, the foreign parties to the transaction must have been vetted by being included on a previously approved license from State or Commerce and consent to an end-use check. This License Exception also broke new ground in requiring that not only the exporter, but also any subsequent reexporter or transferor, must notify any

subsequent consignee of each item shipped under the authority of STA and furnish the ECCN of the item. The consignee must then provide a written statement citing STA, the ECCN, and its agreement to abide by U.S. controls, as well as provide records to BIS upon request. The consignee STA certification requirement thus travels with the item even after reexport or retransfer from the first consignee on its way to ultimate government end use. In this way, the STA can create, in effect, a chain of custody for the item, and the paperwork trail can be followed throughout the 36 countries, thus increasing our ability to monitor and enforce STA-eligible transactions.

Whether an item is exported under a license or license exception, Customs and Border Protection (CBP) agents are reviewing shipping documentation to guard against illicit exports. Similarly, BIS is monitoring export transactions on a daily basis. This effort will be stepped up as a result of STA's application to 600 series items, and we will expect exporters to have available the proper paperwork to adhere to the safeguards under this license exception. In fact, we are actively pursuing our first STA enforcement case in addition to on-going compliance reviews and evaluations of STA transactions.

To ensure that the U.S. Government is not inadvertently impeding legitimate exports of 600 series items while targeting suspicious procurements, BIS began coordinating training with our CBP colleagues on the new changes earlier this month. This training will also extend to other law enforcement partners at Homeland Security Investigations and the Federal Bureau of Investigation over the next three months at local ports and field offices around the country.

On a side note, remember that the 600 series, like the ITAR, has a zero-percent *de minimis* threshold for U.S. arms-embargoed destinations. By eliminating any ambiguity with regard to the application of *de minimis* for 600 series items, BIS is harmonizing the EAR with the ITAR for countries subject to U.S. arms embargoes, including countries subject to anti-terrorism controls, thereby creating a higher fence for military parts and component exports. For all other countries, the EAR's 25% *de minimis* rule will apply for 600 series items.

Another significant regulatory change is the new definition of the term "specially designed." By establishing one definition to cover the term "specially designed" in the EAR to specifically articulate objective criteria for when an item is captured and objective criteria for when an item that initially falls under the definition can

be released, we are making our regulations more transparent and more enforceable. For example, the documentation requirements established in the definition of "specially designed" as it applies to design-intent, will eliminate the need to get into the minds of engineers and require them to document whether an item had non-military design aspirations. This eliminates a sometimes insurmountable obstacle to establishing knowledge in the context of criminal prosecutions.

As part of the "higher fences" initiative, we are also preparing to publish a significant regulatory change to reinvigorate the Unverified List (UVL), which currently imposes a red flag on transaction parties where we have been unable to conduct an end-use check. We are aware of industry's interest in being warned of suspicious foreign actors but also of its concern about the open-ended nature of the UVL and the need for BIS to provide guidance on how to overcome a U.S. Government-imposed red flag. Proposed revisions to the UVL would identify those foreign parties whose bona fides cannot be verified during an end-use check and establish enhanced safeguards for EAR transactions involving such parties. Proposed changes include elimination of license exception eligibility and a requirement - similar to that under License Exception STA - that the exporter

obtain a consignee statement prior to shipment whereby the UVL entity certifies compliance with the EAR and agrees to an end-use check. The export of items not subject to a license requirement (CCL-NLR or EAR99) would need to comply with this new procedure.

We believe this proposal would eliminate the current red flag ambiguity for transactions involving UVL persons and strengthen controls on exports to parties whose bona fides cannot be verified. Use of this list, as in the case of the Entity List, creates a market-based incentive for foreign cooperation with end-use checks and compliance with U.S. export controls.

Finally, as another dimension of ECR, BIS, working with State and Treasury, has established a consolidated screening list to assist you in identifying whether any party to an export transaction requires additional due diligence, from a red flag to a license to a prohibition. The next step is to conduct an assessment of the party yourself, determining whether there is any public information on the party, and whether the requested item appears to be consistent with the proposed end use. For example, if you don't find a company website, that should be a red flag to

seek more information from the company, even if the item is not controlled. This consolidated list contains names on both our Entity List and our Unverified List.

Iranian Transactions and Sanctions Regulations

I want to briefly mention another regulatory development that has implications for the enforcement of U.S. sanctions against Iran. Pursuant to the Iran Threat Reduction and Syria Human Rights Act passed last year, the Treasury Department's Office of Foreign Assets Control (OFAC) amended its regulations, the Iranian Transactions and Sanctions Regulations, in December 2012 to implement expanded sanctions on Iran. One provision in those regulations tightens export controls with respect to knowing re-exports by foreign persons owned or controlled by U.S. persons and authorizes the imposition of liability on those U.S. persons for the foreign persons' conduct. This enhancement of our Iran sanctions provides incentives for U.S. companies to make sure their foreign subsidiaries are not knowingly reexporting EAR99 items to Iran.

Export Control Reform: E2C2 & ITU

Another benefit of ECR is the enhanced enforcement posture of the United States Government through more effective interagency coordination of enforcement efforts. The transfer of munitions items to Commerce actually increases the number of enforcement resources available to monitor compliance. Not only will the same enforcement organizations that already have authority today to monitor defense exports - namely the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) - continue to have authority over such items under the Commerce system, but this effort will be augmented by dedicated Commerce Special Agents and analysts who will assess compliance, including through overseas inspections, conduct criminal investigations, impose administrative penalties and, with the assistance of the Department of Justice, criminal penalties.

This interagency cooperation on export control enforcement has been formalized by the President under Executive Order 13558, establishing the Export Enforcement Coordination Center, or "E2C2." The E2C2 is responsible for enhanced information sharing and coordination between law enforcement and

intelligence officials regarding possible violations of U.S. export control laws. The E2C2 is administratively housed in DHS with a leadership team composed of officials from DHS, the FBI and BIS Export Enforcement.

In addition, within our Office of Enforcement Analysis at BIS, we are hosting the interagency Information Triage Unit, or "ITU." The ITU is responsible for assembling and disseminating relevant information, including intelligence, from which to base informed decisions on proposed exports requiring a U.S. Government license. This multi-agency screening coordinates the reviews of separate processes across the government to ensure that all departments and agencies have a full dataset, consistent with national security, from which to make decisions on license applications. In its first year, the ITU produced more than one thousand analytic products supporting the most sensitive transactions, including those undergoing higher level interagency review. This ensures that licensing officers and policymakers are fully informed about the *bona fides* of parties to proposed export transactions in deciding whether to approve license applications.

Export Control Reform: Administrative Cases

Finally, we are evaluating our methodology for imposing administrative penalties in the context of Export Control Reform with the aim of more closely aligning this process among the three licensing agencies: Treasury, State and Commerce. Industries historically regulated under the ITAR have expressed concern regarding different approaches taken by BIS and the Directorate of Defense Trade Controls (DDTC) at State, particularly with regard to the disposition of voluntary self-disclosures (VSDs). During the past few years at BIS, only a very small percentage of VSDs have resulted in administrative penalties, generally varying from 3 to 6 percent. Only one VSD resulted in the imposition of criminal sanctions – not against the company that submitted it – but against one of its employees: the Gormley case, which I will discuss in a moment.

Both BIS and the Office of Foreign Assets Control (OFAC) at the Treasury Department administer their civil penalty programs under the authority of the International Emergency Economic Powers Act. Under this statue, civil penalties are capped at $250,000, or twice the value of the transaction, whichever is

greater. BIS and OFAC also share enforcement jurisdiction over and closely coordinate on cases involving exports and reexports to Iran, which currently account for almost 40% of our caseload. We are considering updating our Enforcement Penalty Guidelines for our Administrative cases to better align them with the the Guidelines published by OFAC in 2009. As we proceed, we will spell out the details of this initiative in a proposed rule and as always, encourage public comment.

Our objective is not to exercise our authority to hold parties strictly liable for every inadvertent and insignificant violation of the EAR that might take place. Absent evidence of systemic problems recurring over a period of time, inadvertent and insignificant violations will generally be resolved through warning letters. As the munitions items shift from State to Commerce, we will consult with DDTC about the past histories of its registrants and related compliance issues, and take that information into account as we move forward.

Enforcement Cases

As stated previously, all these developments complement our broader, on-going enforcement posture of working to thwart the illegal diversion of U.S.-origin items to prohibited end uses and end users, stressing the importance of internal compliance programs and focusing on the culpability of individuals. As we prepare to issue the first set of final rules implementing the President's reform vision, I want to emphasize that even less-sensitive military items that are moving to the CCL, just like dual-use items and even some purely civil items, can pose serious risks to national security if they fall into the wrong hands.

Although international sanctions have significantly diminished Iran's ability to procure sophisticated dual-use and military items, its complex web of front companies and related financing rings remains a significant threat. This front company network is masked further through the use of transshipment hubs where the sheer volume of trade makes enforcement a challenge. Given Iran's willingness to support terrorist activities through the procurement of unsophisticated electronics and explosive material, the need for extensive domestic and international cooperation is critical.

Today, however, I will highlight some recent notable cases to underscore that our enforcement efforts extend far beyond Iran.

Computerlinks FZCO

In April, 2013, BIS imposed a $2.8 million dollar civil penalty against Computerlinks FZCO, located in the UAE, for charges related to the transfer to Syria of devices designed to monitor and control Internet traffic. In addition to the civil penalty, which is the statutory maximum, the company has agreed to submit to independent, third-party audits.

Computerlinks FZCO provided Blue Coat, the U.S. manufacturer and exporter, with false information concerning the end user and ultimate destination of the items in connection with these transactions. Computerlinks FZCO knew that the items were destined for end users in Syria. However, when placing these orders with Blue Coat, Computerlinks FZCO falsely stated that the ultimate destination and end users for the items were the Iraq Ministry of Telecom or the Afghan Internet service provider Liwalnet. The items subsequently were shipped to

Computerlinks FZCO in the UAE for ultimate delivery to Syria without the required licenses having been obtained.

This statutory maximum penalty reflects the serious consequences that result when companies evade U.S. export controls. Our continuing investigations into the diversion of technology to the Syrian and Iranian governments that can be used to repress their own citizens remains a top priority for Export Enforcement at BIS.

Arc Electronics

Last Fall, the Arc Electronics case resulted in the indictment of 11 individuals and the addition of 165 entities in 12 destinations to the Entity List for their role in illicitly facilitating the export of controlled electronics to Russia. An interagency investigative team that included the FBI, Export Enforcement at BIS, the Department of Justice and the Navy, uncovered a scheme by a Russian military procurement network operating in the United States and elsewhere to illegally export high-tech microelectronics from the United States to Russian military and intelligence agencies. These items are under strict government controls due to their potential use in a wide range of military systems, including radar and

surveillance systems, weapons guidance systems, and detonation triggers. In October of this past year, the indictment was unsealed charging 11 defendants with this illegal export scheme. As Under Secretary Hirschhorn noted, this case is "a perfect example of two of the core benefits of the administration's export control reform effort – higher enforcement walls around controlled items and extensive coordination and cooperation among enforcement agencies."

The Arc Electronics case is important in three regards. First, it exposed an entrenched network of conspirators in the United States that created a front company operating in Texas for the express reason of circumventing U.S. export controls. In fact, the owners went so far as to attend BIS seminars to become experts in how the EAR work. It was tips from the U.S. business community to law enforcement officials that led us to identify this front company organization. Second, it exposed a network of trade facilitation companies in western countries, demonstrating the risks that bad actors are willing to take, and the need for U.S. companies to screen customers even in allied destinations. Third, many companies associated with these transactions are taking steps to change their business practices that will allow their removal from the Entity List, thus demonstrating the value and market-based incentive of the Entity List from a

compliance and enforcement perspective to push companies to establish reputable business practices or risk elimination of U.S. sources of supply.

The Arc Electronics case also highlights our use of the Entity List to target offshore actors engaged in the illegal diversion of U.S.-origin items. The Entity List has become a formidable administrative enforcement tool to identify bad actors; foreign parties that are prohibited from receiving some or all items subject to the EAR unless the exporter secures a license because of the risk these persons pose of diversion of U.S.-origin items to weapons of mass destruction (WMD) programs, terrorism or other activities contrary to U.S. national security and foreign policy interests. In fact, we have found that the Entity List has not only inhibited U.S. exports to destinations of concern, but exports to these countries from other supplier nations as well. In 2012, BIS added 197 new persons on the Entity List, while removing 18.

Gormley

As Under Secretary Hirschhorn stated at the 2010 Update Conference, BIS will step up enforcement efforts "against individuals who flout the rules and against companies whose inadequate internal compliance programs tell us that they are

indifferent to whether they follow the rules." We continue to place an emphasis on individual responsibility. Many times they are one and the same; but on occasion, they are not. We are seeking to punish the willful actor, and once again, a company's commitment to an Internal Compliance Program, or ICP, can be an important factor differentiating a crime of complicity between an individual and his employer, from that of a sole rogue employee.

One such case is the Gormley case, which was opened based on a Voluntary Self Disclosure, or VSD, submitted by Amplifier Research in Souderton, Pennsylvania. Timothy Gormley was an employee of Amplifier Research. Many of this company's products are controlled for national security reasons with application in military systems, requiring a license for export to most destinations outside of Europe. According to his guilty plea, Gormley altered invoices and shipping documents to conceal the correct classification of the amplifiers so they would be shipped without the required licenses, listed false license numbers on the export paperwork, and lied to fellow employees about the status and existence of export licenses. Gormley's actions resulted in at least 50 unlicensed exports of national security items to such destinations as China, India, Hong Kong, Taiwan, Thailand, Russia, and Mexico. In admitting to the conduct, he explained that he was simply

"too busy" to obtain the licenses. The company made the right decision in notifying BIS of the violations and in taking remedial measures. On January 17 of this year, Gormley was sentenced to 42 months in prison, three years of supervised release and a $1,000 criminal fine.

PPG

Another example highlighting the principle of individual and corporate accountability is the PPG case. Xun Wang, a former Managing Director of PPG Paints Trading (Shanghai) Co., Ltd., a wholly-owned Chinese subsidiary of United States PPG Industries, Inc., conspired to export, re-export and transship high performance epoxy coatings to the Chashma II Nuclear Power Plant in Pakistan, a nuclear reactor owned and/or operated by the Pakistan Atomic Energy Commission, which is on BIS's Entity List. Wang was the most senior PPG Paints Trading corporate executive involved in this export scheme. In December 2012, she was sentenced to one year and one day in prison, agreed to pay a $100,000 criminal fine, and ordered to perform 500 hours of community service. She also agreed to pay a $200,000 civil penalty, with another $50,000 suspended, and to be placed on BIS's Denied Persons List for five years, with an additional five years suspended. As Under Secretary Hirschhorn noted, "This case clearly

demonstrates our resolve to hold individuals responsible for violations of our export control laws. Individuals can no longer hide behind a corporate veil."

Wang's cooperation with the government's investigation resulted in a downward variance at her sentencing. It also led to the China Nuclear Industry Huaxing Construction Co., Ltd. guilty plea in December 2012, believed to be the first time a PRC corporate entity pled guilty to export violations in a U.S. court. Huaxing agreed to the maximum criminal fine of $2 million, $1 million of which will be stayed pending successful completion of five years of corporate probation. In addition, Huaxing agreed to pay a civil penalty of $1 million, implement an export compliance program, and conduct annual compliance audits for two years. The company also agreed to a five-year suspended denial of export privileges.

Ericsson de Panama, S.A.

As in the Gormley case, the VSD process is an essential element of any ICP and usually a "great weight" mitigator in a BIS enforcement proceeding. Another case illustrating this point is the Ericsson case. Ericsson de Panama, S.A. of Panama City, Panama, knowingly implemented a scheme to route telecommunications items from and to Cuba through Panama. The scheme included repackaging

items to conceal their Cuban markings, forwarding the items to the United States for repair and replacement, and returning the items to Cuba. In May 2012, Ericsson entered into a settlement agreement with BIS in which it agreed to pay $1.753 million to settle 262 EAR violations. In addition, an independent third party will conduct an audit of all export transactions connected with Cuban customers. By voluntarily disclosing the violations to BIS and the Department of Justice, and cooperating with the resulting investigation, Ericsson was able to avoid criminal prosecution and heavier fines.

Terrorist Organizaiton Procurement Case

Most recently, OEE conducted a joint investigation with the FBI's Philadelphia Joint Terrorism Task Force (JTTF) demonstrating our commitment to preventing unauthorized exports to terrorist organizations on OFAC's SDN list. The target of this investigation engaged in the illegal exportation of both EAR 99 items and items on the CCL to this specially designated terrorist organization. On July 19, 2013, this case resulted in a sentence of 132 months incarceration, 3 years supervised release and a fine of $1,000.00 in connection with a guilty plea entered in April 2012. The target pled guilty to False Statements on an SED,

Conspiracy, Material Support to a Terrorist Organization, Transportation of Stolen Goods, and Passport Fraud.

Compliance and Conclusion

In conclusion, I understand the challenges you face. I've worked in the government and I have practiced in private law firms advising companies on compliance matters. The ECR issues I've discussed today are complicated. And even companies that take export compliance seriously make mistakes. So I know from experience that violations are not always black-and-white.

Our relationship with industry is first and foremost one of cooperation and mutual assistance in facing external challenges to the security of this nation. To help industry avoid mistakes, especially in the context of Export Control Reform, we are redoubling our outreach efforts. We are beginning to boost our visits to companies who will be most affected by the USML to CCL changes, beginning with businesses in the military aerospace industry. As Export Control Reform increasingly affects other sectors, like satellites, military vehicles and electronics, we're going to focus our outreach efforts on them as well. And we are using the

information and tools at our disposal to alert companies of suspicious transactions and parties.

We are doing this for the simple reason that if we can help more companies better understand the regulations and threats, it will benefit both U.S. economic and national security interests. But let me be clear: The best way to ensure you're not violating the regulations is to have a comprehensive internal compliance program in place. A good compliance program pays for itself: it keeps you from committing a violation in the first place; and if you do slip up, it will be a mitigating factor in an administrative penalty proceeding.

Let me also emphasize this point for intangible transfers of technology, including deemed exports - where traditional means of monitoring – for example, shipping documentation and purchase orders – may not apply. In these circumstances, and particularly where there are specific EAR restrictions with regard to certain countries, you need to ensure that conditions can be complied with. This includes knowing what access controls are in place and the efficacy of the technology control plan to prevent unauthorized access on a recurring basis. The illicit re-export of U.S. technology can have more severe national security consequences

than a tangible export, and certainly that may be the case from an intellectual property protection perspective.

Finally, if your company should find itself subject to one of our investigations or enforcement actions, we strongly recommend that you come prepared to explain what compliance procedures you had in place, how things went wrong, and exactly how you have or plan to correct your compliance procedures to prevent problems in the future.

I also strongly encourage you to come forward and file a VSD, informing us of any violations you may internally uncover. A VSD typically results in 50 percent mitigation of the proposed civil penalty if a violation is determined to have occurred. In fact, of the VSD cases resolved in 2011 and 2012, only 3 percent in 2011 and 6 percent in 2012 resulted in the imposition of an administrative civil penalty. We have also made substantial progress at BIS in establishing a more streamlined review process so that those who file VSDs receive a timely response on the disposition of their matter. Most recently, we proposed amending the EAR to include a 180-day deadline for persons who have submitted an initial notification of a VSD to complete and submit the final narrative report to the

Office of Export Enforcement. Our proposed rule was published in November 2012, and we have received helpful feedback from industry. A final rule, responding to public comment, should be published shortly.

And now, let me introduce my colleagues who will serve on our Enforcement panel. Our Moderator Doug Hassebrock, My Acting Deputy and the Director of the Office of Export Enforcement; John Sonderman, the Deputy Director of the Office of Export Enforcement; Kevin Kurland, Director of the Office of Enforcement Analysis; Ned Weant, Director of the Office of Antiboycott Compliance; and Joe Jest of our Chief Counsel's Office.

Thank you for your participation in this conference and your attention today. I wish you all great success with your lawful exports.