

**EXPORT COMPLIANCE: ENSURING SAFETY,
INCREASING EFFICIENCY**

HEARING

BEFORE THE

SUBCOMMITTEE ON TERRORISM,
NONPROLIFERATION, AND TRADE

OF THE

COMMITTEE ON FOREIGN AFFAIRS

HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

—————
MAY 20, 2008
—————

Serial No. 110-202

—————

Printed for the use of the Committee on Foreign Affairs



Available via the World Wide Web: <http://www.foreignaffairs.house.gov/>

—————
U.S. GOVERNMENT PRINTING OFFICE

42-478PDF

WASHINGTON : 2008

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON FOREIGN AFFAIRS

HOWARD L. BERMAN, California, *Chairman*

GARY L. ACKERMAN, New York	ILEANA ROS-LEHTINEN, Florida
ENI F.H. FALEOMAVAEGA, American Samoa	CHRISTOPHER H. SMITH, New Jersey
DONALD M. PAYNE, New Jersey	DAN BURTON, Indiana
BRAD SHERMAN, California	ELTON GALLEGLY, California
ROBERT WEXLER, Florida	DANA ROHRBACHER, California
ELIOT L. ENGEL, New York	DONALD A. MANZULLO, Illinois
BILL DELAHUNT, Massachusetts	EDWARD R. ROYCE, California
GREGORY W. MEEKS, New York	STEVE CHABOT, Ohio
DIANE E. WATSON, California	THOMAS G. TANCREDO, Colorado
ADAM SMITH, Washington	RON PAUL, Texas
RUSS CARNAHAN, Missouri	JEFF FLAKE, Arizona
JOHN S. TANNER, Tennessee	MIKE PENCE, Indiana
GENE GREEN, Texas	JOE WILSON, South Carolina
LYNN C. WOOLSEY, California	JOHN BOOZMAN, Arkansas
SHEILA JACKSON LEE, Texas	J. GRESHAM BARRETT, South Carolina
RUBÉN HINOJOSA, Texas	CONNIE MACK, Florida
JOSEPH CROWLEY, New York	JEFF FORTENBERRY, Nebraska
DAVID WU, Oregon	MICHAEL T. McCAUL, Texas
BRAD MILLER, North Carolina	TED POE, Texas
LINDA T. SÁNCHEZ, California	BOB INGLIS, South Carolina
DAVID SCOTT, Georgia	LUIS G. FORTUNO, Puerto Rico
JIM COSTA, California	GUS BILIRAKIS, Florida
ALBIO SIRES, New Jersey	VACANT
GABRIELLE GIFFORDS, Arizona	
RON KLEIN, Florida	
BARBARA LEE, California	

ROBERT R. KING, *Staff Director*

YLEEM POBLETE, *Republican Staff Director*

SUBCOMMITTEE ON TERRORISM, NONPROLIFERATION, AND TRADE

BRAD SHERMAN, California, *Chairman*

DAVID WU, Oregon	EDWARD R. ROYCE, California
DAVID SCOTT, Georgia,	JOHN BOOZMAN, Arkansas
<i>Vice Chair</i>	TED POE, Texas
RON KLEIN, Florida	DONALD A. MANZULLO, Illinois
GENE GREEN, Texas	THOMAS G. TANCREDO, Colorado
JOSEPH CROWLEY, New York	

DON MACDONALD, *Subcommittee Staff Director*

JOHN BRODTKE, *Subcommittee Professional Staff Member*

TOM SHEEHY, *Republican Professional Staff Member*

KINSEY KIRIAKOS, *Staff Associate*

CONTENTS

	Page
WITNESSES	
Matthew S. Borman, Esq., Acting Assistant Secretary for Export Administration, Bureau of Industry and Security, U.S. Department of Commerce	8
Mr. Todd Owen, Executive Director, Office of Cargo and Conveyance Security, U.S. Customs and Border Protection, U.S. Department of Homeland Security	14
Mark Menefee, Esq., Counsel, Baker & McKenzie	25
Mr. Peter H. Powell, Sr., Senior Counselor, National Customs Brokers and Forwarders Association of America, Inc.	30
Arthur Shulman, Esq., General Counsel, Wisconsin Project on Nuclear Arms Control	33
LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING	
The Honorable Brad Sherman, a Representative in Congress from the State of California, and Chairman, Subcommittee on Terrorism, Nonproliferation, and Trade: Prepared statement	4
Matthew S. Borman, Esq.: Prepared statement	10
Mr. Todd Owen: Prepared statement	15
Mark Menefee, Esq.: Prepared statement	28
Mr. Peter H. Powell, Sr.: Prepared statement	31
Arthur Shulman, Esq.:	
Article from the New York Times by Gary Milhollin and Kelly Motz entitled "Nukes 'R' Us" dated March 4, 2004	36
Prepared statement	39

EXPORT COMPLIANCE: ENSURING SAFETY, INCREASING EFFICIENCY

TUESDAY, MAY 20, 2008

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TERRORISM, NONPROLIFERATION,
AND TRADE,
COMMITTEE ON FOREIGN AFFAIRS,
Washington, DC.

The committee met, pursuant to notice, at 10:04 a.m. in room 2200, Rayburn House Office Building, Hon. Brad J. Sherman (chairman of the subcommittee) presiding.

Mr. SHERMAN. These hearings are being held for a number of reasons, but primarily because of a request by our colleague, Mr. Manzullo, who I am sure will be here expeditiously. I am sure he will be watching the tape and reading the transcript over and over again, as I remind him why these hearings were called.

I am going to yield to our ranking member, Mr. Royce of California, for his opening statement. I will then combine my opening statement and witness introductions.

Mr. ROYCE. I thank you very much, Mr. Chairman. And I think all of us understand that the United States is exporting a larger and larger volume of goods every year. It is part of our economic well-being, and particularly at this time it demands a very vibrant export sector. What we are looking at is how to make that easier.

A very small portion of our exports are problematic, though; and those exports go to countries or individuals that could seek to harm us. And our challenge is to see that the export control system better facilitates the legitimate commerce, while shutting down the trade that could harm our national security.

We know that terrorists and state sponsors of terrorism are actively seeking advanced U.S. technology. We know that from hearings that Chairman Brad Sherman and I have had over the years, looking at such individuals as A. Q. Kahn and the network that he put together.

And it is an increasingly sophisticated procurement network that is evidenced by the type of rogue operations we have seen. So we need a better defense, including improved end-use checks.

The proliferation of weapons of mass destruction technology makes that improvement imperative for us. And the legislation my colleagues have introduced, the focus of this hearing, promises to make life easier for legitimate exporters, and makes it more difficult for the few exporters of illegal goods, including increasing the chances that those individuals that are involved in that kind of activity, are prosecuted.

It prods the bureaucracy into implementing 5-year-old congressional mandates, including synchronizing information on impermissible exports. It aims to improve the effectiveness of U.S. sanctions against rogue regimes, which is all good.

So I look forward to hearing the witnesses' views. And while welcoming this legislation, I would like to hear how it might work in the bureaucratic depths. Oftentimes what looks good on paper here doesn't translate all that well in practice.

And, moreover, bureaucratic ineptitude is common. It is a given. And computer modernization hasn't been a government forte. So we should be asking questions, which we will do today, in order to try to examine that aspect of the problem.

Thank you, Chairman Sherman.

Mr. SHERMAN. Thank you, Ranking Member Royce. The subcommittee today will focus on ensuring compliance with the various export controls and embargoes imposed on American exports to help protect our national security and advance our foreign policy interests.

Of course, these rules also have other objectives, including statistics about our exports. But those objectives are pretty much outside the scope of the Foreign Affairs Committee.

Export rules are developed, administered, and enforced by a dozen or more agencies. It is a complicated maze of regulations and overlapping jurisdictions. The twin goal of our subcommittee's work has been to increase efficiency, while ensuring that we have adequate control of technologies that can threaten our security.

Last year we held hearings on the licensing process for munitions and dual-use items. We found that the State Department's Directorate of Defense trade controls had inadequate resources and inadequate staffing to review commercial licenses for military exports in a timely and thorough manner.

In response, this subcommittee worked in a bipartisan manner to draft legislation that helps reform our licensing process in a way that protects our national security while improving processing times. Earlier this month the full House of Representatives passed our legislation as part of the Security Assistance and Arms Export Control Act of 2008. I want to thank Mr. Manzullo, who will be properly chided when he arrives, along with Mr. Royce, Chairman Berman, and Ranking Member Ros-Lehtinen, for working with me on this important legislation.

Today, we turn our attention to export control compliance to examine how the U.S. Government ensures compliance with export controls and embargoes from the point of shipment to the final destination of exports, and in some cases through conduits, which may be the first foreign buyer to subsequent foreign buyers.

This is a serious national security concern, and directly affects our non-proliferation exports. The case in point is that of Mohammed Farahbaksh. For over a decade, this individual smuggled United States goods to help Iran's nuclear program. Beginning in 1997, he started selling United States computer parts to a branch of the Iranian Government working on Iran's ballistic missile system. He continued delivering United States parts to the Iranian missile program until 2004. He even went so far as to sell a com-

munications systems that is on the Commerce Control list to an Iranian-owned oil tanker.

He did this through transshipment and diversion chiefly with companies that he owned in the United Arab Emirates. He shipped the goods to his companies in the UAE, and from there, they were sent to Iran. He was caught in 2004, thanks to the efforts of special agents at the Department of Commerce and Homeland Security, and has admitted his guilt.

This focuses our attention on the Port of Dubai, the seventh-largest container port in the world. And it has become a center for the illegal transshipment of sensitive technology.

I want to compliment all Members of Congress because it was this branch of government that caused Dubai not to be in control of our ports. Clearly, if that decision had been left just to the Executive Branch, Dubai would control more ports than just those in the UAE.

The administration took some important steps to take transshipments from Dubai more seriously in 2005. Dubai signed on to a moratorium of understanding with the United States, making the UAE the first government to participate in an initiative intended to detect and seize radioactive materials. In 2007, the administration threatened to designate the UAE a country of concern for diversion of WMD-capable exports.

By April of last year, the UAE had approved a new law strengthening export controls. Within months, 40 firms involved in dual-use exports to Iran and other countries had been shut down.

Given this history, it is amazing that the administration initially approved the Dubai Ports deal. But that is an aside, not relevant directly to the hearings in front of us.

Given the serious threat of the Iranian nuclear program, we must increase our efforts. There is still only one export control officer stationed in the UAE designated to conduct end-use checks, and that one person is only one of five such individuals worldwide.

I have sought to further restrict trade with Iran, as have many members of our full committee and this subcommittee and to stop U.S. firms from doing business with Tehran through their subsidiaries. Countries that fail to adequately address transshipment of U.S. technology should also be prodded. If necessary, we should be talking about sanctions.

There is a clear need for clarity. One of the options available to us is embodied in H.R. 5828, which is in part the focus of today's hearings. When one properly faces the clarity of prohibitions, this relates to Iran and other countries, the best licensing system in the world, and the tightest restrictions are meaningless without the ability to ensure that exporters are following the law, and that the expectations of the system are transparent to U.S. business.

I could reveal the other provisions of H.R. 5828, but why would I do that in the absence of its fine author, who will be with us soon?

We need to focus on other aspects of our export control system. And I look forward to hearing from our witnesses.

With that, I will yield for an opening statement to Mr. Poe.

[The prepared statement of Mr. Sherman follows.]

Subcommittee on Terrorism, Nonproliferation and Trade
Export Compliance: Ensuring Safety, Increasing Efficiency
May 20, 2008

Opening Statement
of
Chairman Brad Sherman

The Subcommittee today will focus on ensuring compliance with the various export controls and embargos imposed on American exporters to help protect national security and advance the foreign policy interests of the United States.

Export rules are developed, administered and enforced by a dozen or more agencies. It is a complicated maze of agencies and regulations. The twin goals of our Subcommittee's work have been to increase efficiency while ensuring that we have adequate controls on the technology that can threaten our security.

Past Work

Last year, we held a hearing on the licensing process for munitions and dual use items.

We found that the State Department's Directorate of Defense Trade Controls had inadequate resources and staff to properly review commercial licenses for military exports in a timely and thorough manner.

In response, this Subcommittee worked in a bipartisan manner to draft legislation to help reform our licensing process in a way that protected national security while improving the review time for legitimate U.S. exports.

Earlier this month the Full House of Representatives passed our legislation as part of the Security Assistance and Arms Export Control Reform Act of 2008.

I want to thank Mr. Manzullo, Mr. Royce, Chairman Berman and Ranking Member Ros Lehtinen for working with me on this important legislation.

Today, we turn our attention to export control compliance to examine how the U.S. government ensures compliance with export controls and embargoes from the point of shipment to the final destination of the exports.

This is a serious national security concern and critical to our nonproliferation efforts.

The Case of Mohammad Farahbaksh

The story of Mohammad Farahbaksh illustrates this extremely well.

For over half a decade, Mr. Farahbaksh smuggled U.S. goods to help Iran's nuclear program.

Beginning in 1997, he started selling U.S. computer parts to the Shahid Hemmat Industrial Group, which is a branch of the government in Tehran working on Iran's ballistic missile program.

Mr. Farahbaksh continued supplying U.S. parts and components to the Iranian missile program until 2004.

He even went so far as to sell a communications system that is on the Commerce Control List to an Iranian owned oil tanker.

How did he do it?

It was a classic case of transshipment and diversion.

Mr. Farahbaksh who was an Iranian national and a U.S. citizen that partly owned two UAE based companies: Diamond Technology LLX and Akeed Trading Company.

He shipped the goods to his companies in the UAE, and from there sent them on to Iran, just a stone's throw away.

He was caught in 2004 thanks to the efforts of Special Agents at the Departments of Commerce and Homeland Security.

Mr. Farahbaksh admitted his guilt a few weeks ago; however, he is not an anomaly.

The UAE and the Threat of Transshipment

The Port of Dubai is the seventh largest container port in the world, and it has become a center for the illicit transshipments to sensitive technology. The administration has taken some important steps to take transshipment from the UAE more seriously.

In 2005, Dubai signed a Memorandum of Understanding with the U.S., making the UAE the first government in the Middle East to participate in an initiative intended to detect and seize radioactive materials.

In 2007, the Administration threatened to designate the UAE as a “country of concern for diversion” of WMD capable exports.

By April of last year, the UAE has approved a new law strengthening export controls, and within months 40 firms involved in dual use exports to Iran and other countries were shut down.

But given the seriousness of the threat of the Iranian nuclear program, we must increase our efforts.

There is still only one export control officer stationed in the UAE designated to conduct end use checks, and that person is one of only 5 such individuals worldwide.

I have sought to further restrict trade with Iran, and stop U.S. firms from doing business with Tehran through their subsidiaries. Countries that fail to adequately address transshipment of US technology should be targeted themselves for sanctions.

The Need for Clarity – H.R. 5828

One problem we face is clarity in the prohibitions. This relates to Iran and to other countries.

The best licensing system in the world and tightest restrictions are meaningless without the ability to ensure that exporters are following the law and that the expectations of the system are transparent to American businesses.

We have approximately a dozen lists created by three agencies: The Departments of Commerce, Treasury, and State, that identify parties to which you cannot ship various goods and technology.

Exporters and shippers turn to commercial databases that seek to keep up with the changes in these lists. But this should be a federal government responsibility – the creation of a single comprehensive list to ensure that exporters can easily comply.

Two of my colleagues Reps. Manzullo and Smith have introduced relevant legislation: HR 5828, *The Securing Exports Through Coordination and Technology Act*.

This bill would require the Department of Commerce to work across the bureaucracy to integrate our export control lists into the Automated Export System, the electronic filing system for exporters. It would also make use of that system mandatory and require for users of the system to be licensed to ensure that they are trustworthy and know how to use the system.

This system should allow exporters to verify that a shipment is legal; it would gather valuable data on controlled items and technologies, and make the compliance checks

more efficient. If all of its data is preserved – i.e., if attempted filings, filings that were ultimately prohibited or preserved– it should prove as an important prosecutorial tool as well.

The burden of implementing this legislation falls most heavily on the Department of Commerce, and we have asked the Census Bureau to submit written testimony on how it would manage the data collection requirements of the bill. However, Commerce’s Bureau of Industry Security and the Department of Homeland Security will utilize the system to ensure compliance with various export controls – and thus these two agencies are represented here today.

We look forward to hearing from our two government witnesses how this proposed change would impact day to day review of export compliance at our ports and beyond.

Review of Enforcement Authority

Additionally, we must look at the ability of the administration to investigate cases of wrong doing and bring offenders to justice.

The Bureau of Industry and Security is supporting legislation which would reauthorize the Export Administration Act (EAA), which provides the authority for the control of dual use items. The EAA has been expired since 2001, and our control over dual use items has been imposed by regulatory fiat under IEEPA ever since.

We are aware that BIS would like us to consider the “Export Enforcement Act” which would extend the Export Administration Act of 1979 for 5 years, while adding a number of new enforcement provisions. Perhaps most importantly for the purposes of this hearing today, the Bureau of Industry Security is seeking through this legislation law enforcement status for their agents, as status that expired with the EAA.

The Senate has already introduced this legislative package, S. 2000, the Export Administration Act of 2007.

I understand that members of this Subcommittee and the Full Committee are taking a serious look at introducing legislation in the House, and I look forward to working with them. I hope that we can accomplish many of the goals of the Manzullo-Smith bill, as well as the Administration’s package in the coming weeks.

Conclusion

Ensuring a strong and efficient export compliance system is critical to both U.S. national security and the success of American businesses.

I look forward to our witnesses’ testimony today on this important matter.

Mr. POE. Thank you, Mr. Chairman. I will yield back. I will just ask questions to our panel. Thank you.

Mr. SHERMAN. We want to welcome our two panelists. The first is Matthew Borman, acting assistant secretary for export administration at the Bureau of Industry and Security, the Department of Commerce. He is responsible for implementing the Bureau's controls on export of dual-use items in order to achieve our national security objectives.

I will also welcome Mr. Todd Owen, the executive director of the Cargo and Conveyance Security Office within the U.S. Customs and Border Protection Office of Field Operations. As the executive director for cargo and conveyance security, having held that position since May 2006, Mr. Owen is directly responsible for our cargo security programs and policies of Customs and Border Protection.

With that, Mr. Borman.

Mr. Smith, do you have an opening statement, or would you just—

Mr. SMITH. No.

Mr. SHERMAN. Okay.

STATEMENT OF MATTHEW S. BORMAN, ESQ., ACTING ASSISTANT SECRETARY FOR EXPORT ADMINISTRATION, BUREAU OF INDUSTRY AND SECURITY, U.S. DEPARTMENT OF COMMERCE

Mr. BORMAN. Thank you, Mr. Chairman, distinguished members of the committee. I appreciate the opportunity to discuss the Department of Commerce's role in the export control compliance regime and the proposed legislation, H.R. 5828, Securing Exports Through Coordination and Technology Act.

I would like to summarize the written testimony I have submitted for the record.

In the post-9/11 era, ensuring our dual-use export controls are effective and efficient is an increasingly challenging task. At the Bureau of Industry and Security, we strive to ensure that our controls address both the varied and diffuse security threats and the competitive challenges presented by globalized technologies and markets.

We continually evaluate and update our export licensing—

Mr. SHERMAN. Mr. Borman, if you can speak a little closer to the microphone. Everyone in this room wants to hear every word.

Mr. BORMAN. We continue to address both the varied and diffuse security threats, and the competitive challenges presented by the globalized technology markets.

We continually evaluate and update our export licensing compliance and enforcement processes to support the continued technology leadership, economic power, and national security of the United States.

The Bureau has extensive cooperation with other departments and agencies and U.S. industry in carrying out its mission. We cooperate closely with the Departments of Defense, Energy, and State, and the intelligence community in making policy, establishing jurisdiction, and setting control levels for technology and reviewing export license applications.

We also have data-sharing arrangements with the Census Bureau for access to the Automated Export System data, as well as the Department of Homeland Security for access to the Automated Targeting System to facilitate compliance. We also work closely with a number of agencies, including the Departments of Justice and Homeland Security, in actually enforcing our dual-use export controls.

Once an export license application is submitted to BIS, it is reviewed by policy and enforcement experts at the Bureau, as well as experts at Defense, Energy, State, and compared to classified intelligence information to determine whether to approve or deny the application.

Part of review may entail an in-country pre-license check of foreign parties to the application. Once a license is approved, follow-up to ensure compliance can include an in-country post-shipment verification, review of AES data, and monitoring of adherence to reporting requirements in the license.

AES plays a vital role in the administration and enforcement of our regulations. We are working with Census and Customs and Border Protection to enhance the AES system. For example, on April 28, AES established new fatal errors—which means exports cannot be made—when a license exception symbol is not accompanied by the required export control classification number. With this change, we expect that exporter compliance with the license exception requirement of our regulations will increase substantially over the next 2 years.

We are continuing to explore additional AES validations that could be implemented in a cost-effective manner to further improve compliance prior to shipments occurring.

AES data also supports our investigative functions. Our special agents and analysts routinely access AES data through the Automated Targeting System, which is a criteria-specific searchable database.

ATS, the Automated Targeting System, has proven to be a very valuable tool for BIS, and has generated both criminal and administrative investigations. It is also very valuable in ongoing investigations to develop additional leads and/or identify associates of suspected companies.

For example, a BIS special agent recently identified a United States company attempting to export a milling and cutting machine to China without the required license. The item was detained, and the ensuing investigation uncovered additional violations.

While the AES electronic filing requirements have provided BIS with much important information regarding the export of controlled goods, AES also has its limitations. BIS welcomes the broad goals of H.R. 5828 to enhance the reliability and effectiveness and information in AES.

We have identified some technical revisions to the bill, which are detailed in my written testimony.

I look forward to working with your staff on the bill to ensure that any modifications to the AES system are precise and cost-effective.

In situations where there has not been full compliance with the U.S. dual-use export control regime, it is critical that BIS have the

full necessary range of authorities to enforce the statute and the regulations. The major activities of BIS's enforcement program include investigating criminal and administrative violations, and imposing civil sanctions for violations of the regulations.

A significant challenge for BIS, especially with respect to its enforcement activities, is the longstanding lapse of the Export Administration Act of 1979, as amended. While in lapse, the EAA cannot be updated; and thus, the enforcement authorities of BIS special agents have not kept pace with an ever-changing criminal landscape.

S. 2000, the Export Enforcement Act of 2007, sponsored by Sen. Christopher Dodd, addresses this challenge, by enhancing BIS's enforcement authorities, including authority for our agents to work directly with foreign counterparts and conduct undercover operations in the United States.

We support prompt enactment of this bill, which is similar to the administration's proposal, to address one of the most significant challenges BIS faces in administering the dual-use export control system. Use of all possible tools, including the AES system and a re-authorized EAA, is critical for most effectively meeting the unprecedented security and economic challenges in today's world.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Borman follows:]

PREPARED STATEMENT OF MATTHEW S. BORMAN, ESQ., ACTING ASSISTANT SECRETARY FOR EXPORT ADMINISTRATION, BUREAU OF INDUSTRY AND SECURITY, U.S. DEPARTMENT OF COMMERCE

Mr. Chairman, distinguished members of the Committee, thank you for the opportunity to discuss the Department of Commerce's role in the export control compliance regime and the proposed legislation, H.R. 5828, *The Securing Exports Through Coordination and Technology Act*.

In the post-9/11 era, ensuring our dual-use export controls are effective and efficient is an increasingly challenging task. At the Bureau of Industry and Security (BIS), we strive to ensure that our controls address the varied and diffuse security threats and competitive challenges our nation faces. We continually evaluate and update our export licensing, compliance, and enforcement processes to support the continued technology leadership, economic power, and national security of the United States.

Licensing

As has been detailed in previous testimony and hearings, BIS has a robust program for controlling appropriate technologies, vetting export license applications, and informing U.S. companies of their obligations under the Export Administration Regulations (EAR). BIS carries out this robust program in cooperation with a number of other departments and agencies and U.S. industry. BIS cooperates closely with the Departments of State, Defense, and Energy, and the intelligence community in making policy, establishing jurisdiction and setting control levels for technology, and reviewing export license applications.

Over the past ten years, BIS has received between 10–20,000 license applications per year, with the highest amount over that period being Fiscal Year 2007 with a total of 19,296 applications received. Under Executive Order 12981, the Departments of State, Defense, and Energy can review all export license applications submitted to BIS. Defense and State review about 80% of all such license applications and Energy reviews about 34%. The average processing time for all BIS licenses in FY 2007 was 28 days.

In addition to the interagency review process, BIS further assesses prospective and retrospective compliance through end-use checks. When performed prior to approval (pre-license check), the check provides feedback on the reviewing agencies' initial recommendation to approve a particular transaction. When performed after an item is delivered, the results of a post-shipment verification provide direct feedback on the effectiveness of the license review process. BIS conducted over 850 end-use checks in over 80 countries in FY 2007.

Outreach

In addition to the licensing process, BIS conducts other activities to assess and facilitate compliance with the EAR. One such activity is industry outreach. Informing U.S. companies, and their foreign partners, of the requirements under the EAR is critical to facilitating compliance. Industry cannot comply with regulations it does not understand or know exist. BIS typically conducts approximately 45 live seminars annually across the United States and in two to three countries abroad each year. BIS identifies attendees using licensing and export data and evaluates the effectiveness of these seminars through detailed evaluation forms from participants. Moreover, BIS has recently established an on-line training room on its website for individualized, cost-effective outreach to individuals and small- and medium-sized enterprises in the United States and around the world. The on-line training room has already received over 10,000 hits from interested internet users. BIS also offers webinars and other on-line materials and tutorials to aid in its outreach efforts and participates in related outreach events organized by other agencies and entities. BIS also participates in related outreach events organized by domestic and foreign industry as well as other agencies.

Export Data

Other compliance activity is based on data sharing arrangements with the Census Bureau (Census) for data in the Automated Export System (AES) and the Department of Homeland Security (DHS) for accessing data in the Automated Targeting System (ATS).

BIS uses AES data to verify compliance with the EAR. AES is the system for filing required data on exports from the United States and is the basis for U.S. foreign trade statistics. AES also helps detect and prevent the export of certain critical technology and commodities to unauthorized destinations or end users by targeting and identifying suspicious shipments prior to shipment. AES was implemented on July 3, 1995, to automate the manual process of filing the Shipper's Export Declaration (SED) and Outbound Carrier Manifests. AES is a joint, cooperative project supported by Census and DHS' Customs and Border Protection (CBP) and used by BIS and the Department of State's Directorate of Defense Trade Controls (DDTC). Since its inception, AES has served as an information gateway for Census, CBP, BIS and DDTC to improve the reporting of export trade information, customer service, compliance with and enforcement of export laws, and provide paperless reports of export information. BIS is continually working with Census and CBP to refine AES validations to further enhance export control administration.

For export transactions subject to BIS control, AES works as follows: Prior to export, exporters, with a few exceptions, are required to make AES filings electronically, providing approximately 36 different data elements, including the item, consignee, description of the item, country, quantity and value. AES performs edits and validations on this data, and exporters either receive error messages or an AES certification number upon a successful submission. For items subject to a licensing requirement, exporters must also identify the license number or license exception symbol and export control classification number (ECCN). For such items, relevant information regarding the export is transferred from BIS to CBP nightly every Tuesday through Saturday through a dedicated and secure line. Following the actual export of the item, CBP then notifies BIS within 24 to 48 hours of the shipment under the relevant BIS individual license, which is input into BIS' licensing system. BIS also receives a separate AES file from Census that is reconciled with data in ECASS to validate whether exports shipped under a license or license exception are consistent with the respective authorizations. Those that are not reconciled are referred to BIS' Office of Export Enforcement for investigation.

Furthermore, BIS is working with Census and CBP to enhance AES validations. For example, on April 28, BIS established new fatal errors in AES when a license exception symbol is not accompanied by an ECCN. We expect that exporter compliance with this license exception requirement of the EAR will increase from approximately 85% in fiscal year 2007 to 97% in 2010. We are continuing to explore additional validations to AES (and any successor system) that could be implemented in a cost-effective manner to further improve compliance prior to shipments.

Enforcement

BIS also works closely with a number of agencies, including the Department of Justice and DHS, to enforce its dual-use export controls. BIS uses AES data to support BIS' investigative functions. BIS Special Agents and analysts routinely access AES data through ATS. ATS is a criteria-specific searchable database. ATS has proven to be a valuable tool for BIS and has generated both criminal and adminis-

trative investigations. It is also valuable in ongoing investigations to develop additional leads and/or identify associates of suspect companies.

For example, ATS/AES data were instrumental in a BIS investigation that led to the identification of a major diverter of U.S.-origin aircraft parts to Iran. Upon receiving information about a suspect foreign company, an ATS search identified numerous U.S. companies exporting to the suspect overseas company. When the U.S. companies were interviewed, BIS learned that the overseas company had previously been in business under a different name that had been on the BIS Denied Parties List; the company had changed its name and continued to violate the Iranian Transaction Regulations and the BIS Denial Order. BIS advised the unwitting U.S. companies to not conduct business with this overseas firm, thus preventing future violations, and the new alias was added to the BIS Denied Parties List.

In another example, a BIS Field Office Special Agent identified a U.S. company exporting a milling and cutting machine destined for China without a BIS license. As many milling machines require export licenses, the item was detained and subsequently determined to require an export license. The ensuing investigation uncovered additional violations.

H.R. 5828

The above examples demonstrate the utility that AES provides with regard to BIS' compliance and enforcement efforts. BIS welcomes the broad goals of H.R. 5828 to further enhance the reliability and effectiveness of information in AES. However, given the complexities of the EAR and law enforcement needs, there are limitations to the types of validations that can be programmed into AES. In fact, some recent experience with creating new requirements in AES demonstrates that making changes to the system as proposed by H.R. 5828 will require significant resources for implementation, both initially and on an on-going basis.

BIS looks forward to working with the Subcommittee on making this bill as productive and fruitful as possible. With this background, BIS provides detailed comments to the proposed manager's amendment to H.R. 5828. While Census' testimony for the record pertains to the licensing, outreach, and data sharing elements of H.R. 5828, the following BIS comments focus on the export control provisions in the bill:

- *Section 3, amending 13 U.S.C. § 305 (a)*. Because certain requirements in § 305(c) permit the filing of data when a transaction may violate the restrictions of the EAR (i.e., a compliance alert or other warning, not a fatal error), the language in § 305(a) needs to be amended for consistency purposes.
- *Section 3, amending 13 U.S.C. § 305 (b)*. BIS publishes many revisions to the EAR annually. Requiring Commerce to make changes to AES to reflect EAR revisions could add significant time and cost to the rulemaking process. BIS would have to coordinate with Census and CBP in advance of any rulemaking to determine the feasibility of inputting new requirements into AES. In addition, any change to AES will have cost implications. While BIS routinely reviews EAR revisions to determine how best to implement and enforce them, including through AES, mandating such action could adversely impact national security when rules require immediate publication or if the Department does not have resources to incorporate EAR changes into AES.
- *Section 3, amending 13 U.S.C. §§ 305 (c)(1) and (c)(3)(A)*. There is not a one-to-one correlation between Harmonized Tariff System (HTS) and ECCN codes. In fact, HTS codes routinely are associated with multiple ECCNs and ECCNs are routinely associated with multiple HTS codes. While HTS codes could provide exporters with limited assistance in classifying an item on the Commerce Control List, using AES to electronically alert filers of a potential link under (c)(1) would be confusing and potentially lead to a large number of false positives. Issuing compliance alerts under (c)(3)(A) would be even more problematic as they could inhibit exporters from proceeding with a transaction, thereby impeding legitimate trade. Moreover, BIS uses AES compliance alerts for enforcement purposes, and this provision could unnecessarily target legitimate trade and waste BIS resources.
- *Section 3, amending 13 U.S.C. § 305 (c)(2)*. Implementing screens for parties on the Entity List would be very complicated and time-consuming. Supplement No. 4 to Part 744 of the EAR identifies both specific entities and subordinate entities that can include any entities, institutes, or centers associated with those entities, but not explicitly identified. In addition, there is no standard list of items for which an exporter must seek a license. For some entities, a license is required for all items subject to the EAR; for others, a license is required only for specific ECCNs or computer tiers. Programming and keep-

ing such disparate lists up to date in AES to ensure that appropriate transactions receive a fatal error would be virtually impossible.

When effectively used, AES can minimize the number of technical reporting errors (e.g., keystrokes) and allow BIS to focus its compliance and especially its enforcement resources on issues of national security concern. The major activities of BIS' enforcement program include investigating criminal and administrative violations and imposing civil sanctions for violations of the EAR, the International Emergency Economic Powers Act (IEEPA), as amended by the International Emergency Economic Powers Enhancement Act (IEEPEA), the Chemical Weapons Convention Implementation Act (CWCIA), and related statutes and regulations. Consistent with the President's national security priorities, BIS prioritizes its enforcement activities on cases relating to the proliferation of weapons of mass destruction, terrorism, and military diversion. In FY 2007, BIS Special Agents made 23 arrests, and assisted in obtaining 16 convictions and \$25.3 million in criminal fines. Administratively, 65 cases were settled through Final Orders totaling \$5.8 million in fines.

Export Administration Act

A significant challenge for BIS, especially with respect to its enforcement activities, is the long-standing lapse of the Export Administration Act of 1979, as amended (EAA). This lapse hinders the ability of BIS to employ up-to-date authorities to enforce the dual-use export control system. While in lapse, the EAA cannot be updated and thus the enforcement authorities of BIS Special Agents have not kept pace with an ever changing criminal landscape.

Although BIS enforcement efforts would benefit from an improved AES system, it is vital that BIS Special Agents acquire updated enforcement authorities to combat proliferation in an era of globalization. For example, BIS' agents are currently unable to work directly with their foreign law enforcement counterparts. In addition, they do not have the authority to conduct undercover operations—or even make a simple arrest—in *the United States* without undergoing a cumbersome bureaucratic process. While effective cooperation between U.S. law enforcement agencies has enabled our agents to overcome some of these hurdles, they need updated enforcement authorities to enhance our national security by enabling domestic and international investigations and enforcement actions to proceed more quickly, efficiently, and effectively.

The Administration has been working with Congress since 2001 to renew the EAA in order to strengthen the dual-use export control system. With the EAA in lapse, dual-use export controls have been kept in place by annual Executive Orders invoking IEEPA.

When the IEEPA is invoked, its penalties are applied to dual-use export control violations. Though those penalties have been increased by the enactment of the IEEPEA, they are not as strong as those proposed by the Export Enforcement Act (S. 2000). Additionally, as a result of this unique structure for the continuation of export controls, prosecutors are sometimes reluctant to bring criminal indictments for export control violations given the complex web of authorities for current export control regulations.

S. 2000, the "Export Enforcement Act of 2007," sponsored by Senator Christopher Dodd, would reauthorize the EAA and enhance the enforcement authorities of BIS Special Agents. We support prompt enactment of this bill by the Senate, which is similar to the Administration's proposal, and would address one of the most significant challenges BIS faces in administering the dual-use export control system.

Conclusion

The United States faces unprecedented security challenges from threats of terrorism to proliferation of weapons of mass destruction and advanced conventional weapons to instability in a number of regions in the world. The United States also faces unprecedented economic challenges from the increasing worldwide diffusion of high technology and global markets. Enactment of S. 2000 is essential to being able to enforce the EAR. In addition, H.R. 5828, as revised per Department of Commerce comments, will be another important tool needed to meet these threats.

Mr. SHERMAN. Thank you. I should point out that originally scheduled to testify before us was Mr. Ralph Basham of the Department of Homeland Security. He is, of course, the Commissioner of Customs and Border Protection.

They then decided to substitute a man who reports to Mr. Basham, Mr. Robert Jacksta, who is the Deputy Assistant Commissioner. And then when they found out that these hearings were re-

quested by Mr. Manzullo, they decided that they needed to send someone who reports to Mr. Jacksta, a fine individual here, Mr. Todd Owen, who is pinch-hitting for his boss's boss, and will do a spectacular job because he can tell us what is really going on. And don't tell us the administration line. It doesn't go beyond this room. [Laughter.]

STATEMENT OF MR. TODD OWEN, EXECUTIVE DIRECTOR, OFFICE OF CARGO AND CONVEYANCE SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. OWEN. Thank you. Good morning, Chairman Sherman, members of the subcommittee. It is an honor to appear before you today to discuss the role that U.S. Customs and Border Protection plays in enforcing U.S. export laws and regulations.

And again, let me begin by apologizing to the subcommittee and to my fellow witness for the last-minute substitution. Deputy Assistant Commissioner Jacksta was called away today to appear at some meetings down in Mexico City with Commissioner Basham. So CBP does apologize for this late change.

My testimony today will focus on the role U.S. Customs and Border Protection (CBP) plays in enforcing U.S. export laws and regulations, inspecting and examining cargo and export documentation, detaining questionable shipments, seizing shipments in violation of export control laws, and interdicting unreported currency, stolen vehicles, and other illegal exports.

As America's frontline border agency, CBP employs highly trained and professional personnel, resources, expertise, and law enforcement authorities to meet our twin goals of improving security and facilitating the flow of legitimate trade and travel.

In support of DHS's goal of keeping terrorists from acquiring weapons of mass destruction or of mass effect, other weapons and weapon components, CBP officers and special agents with U.S. Immigration and Customs Enforcement, ICE, work together to ensure that unauthorized exports are not allowed to leave the country. This includes the enforcement of the U.S. munitions list, the dual-use list, controlled nuclear materials and technology, and sanction or trade embargoes.

CBP is the last line of defense in the export control process, as CBP can execute its broad border-search authority as the authority to enforce export control regulations. It is physically located at the borders of our nation's ports of entries, and it has the ability to inspect, search, detail, and seize goods being exported illegally or without the proper authorizations, licenses, or license exemptions.

The key to effective export controls is the collection and screening of export transactional information by a law enforcement agency prior to the departure of the cargo from the U.S. The Automated Export System (AES) was first developed by the U.S. Customs Service, now CBP, with the assistance of the U.S. Census Bureau in 1995 to collect export transaction information for statistical and law enforcement purposes. AES continues to be a key tool for CBP today.

Our outbound enforcement targeting module in CBP's Automated Targeting System helps us to identify and target exports which are

high risk for export violations. When licensing issues arise, we work with ICE's Exodus Command Center, a single point of contact for CBP officers and ICE special agents in the field which provides operational support from national export licensing authorities.

CBP's long-term objective is to fully integrate U.S. exports into the International Trade Data System Initiative (ITDS). ITDS was legislatively recognized by the Safe Port Act of 2006, and is an information technology initiative that aims to provide a single window for the international trading community to provide data to the government for import and export transactions. Census is a participating agency in the ITDS initiative.

CBP is the lead agency for the integration of participating government agencies under the ITDS umbrella, and the ultimate goal is full interoperability of all automated systems relative to exchanging and sharing transaction data.

CBP's frontline officers and agents working in coordination with ICE special agents will continue to protect America from terrorist threats, while executing our traditional enforcement missions in immigration, customs, and agriculture, while balancing the need to facilitate legitimate trade and travel.

These initiatives discussed today are only a portion of DHS's efforts to secure our homeland, and we will continue to provide our men and women on the front lines with the necessary tools to the system in protecting our nation.

I would like to thank Chairman Sherman, members of the subcommittee, for the opportunity to present this testimony today. And again, I do apologize for the witness substitution, and would be happy to answer any questions.

[The prepared statement of Mr. Owen follows:]

PREPARED STATEMENT OF MR. TODD OWEN, EXECUTIVE DIRECTOR, OFFICE OF CARGO AND CONVEYANCE SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, U.S. DEPARTMENT OF HOMELAND SECURITY

CHAIRMAN SHERMAN, RANKING MEMBER ROYCE AND DISTINGUISHED SUBCOMMITTEE MEMBERS.

My testimony this morning focuses on the role of the U.S. Department of Homeland Security (DHS) in enforcing U.S. export laws and regulations, inspecting and examining cargo and export documentation, conducting criminal investigations relating to illegal exports, detaining questionable shipments, seizing shipments in violation of export control laws, and interdicting unreported currency, stolen vehicles, and other illegal exports.

I am here to represent DHS; however, I am the Deputy Assistant Commissioner for the Office of Field Operations at US Customs and Border Protection (CBP). My testimony includes information on how CBP and Immigration and Customs Enforcement (ICE) work together to address export compliance. In saying this, my area of expertise is with CBP operations and I will not be able to address questions regarding ICE operations. I will be happy to take back any ICE questions and have them submit answers for the *Congressional Record*.

As America's frontline border agency, CBP employs highly trained and professional personnel, resources, expertise and law enforcement authorities to meet our twin goals of improving security and facilitating the flow of legitimate trade and travel. CBP is responsible for preventing terrorists and terrorist weapons from entering the United States; apprehending individuals attempting to enter the United States illegally; stemming the flow of illegal drugs and other contraband; protecting our agricultural and economic interests from harmful pests and diseases; safeguarding American businesses from theft of their intellectual property; regulating and facilitating international trade; collecting import duties; and enforcing United States trade laws.

On a typical day, CBP processes more than 1.13 million passengers and pedestrians; 70,200 truck, rail, and sea containers; 251,000 incoming international air

passengers; 74,100 passengers and crew arriving by ship; and 82,800 shipments of goods approved for entry. CBP also collects \$88.3 million in fees, duties and tariffs and makes 70 arrests of criminals at our Nation's ports of entry and 2,402 apprehensions between the ports of entry per day. Also, each day CBP and ICE seize an average of 7,388 pounds of narcotics, \$652,603 worth of fraudulent commercial merchandise, 41 vehicles, 164 agriculture pests, and 4,296 prohibited meat or plant materials.

In support of DHS's goal of keeping terrorists from acquiring weapons of mass destruction, weapons of mass effect, other weapons, and weapon components, CBP officers and ICE special agents work together to ensure that unauthorized exports are not allowed to leave the country. This includes the enforcement of the U.S. Munitions List, the Commerce Control List (i.e. items that can be used for both civilian and military purposes), controlled nuclear materials and technology, and sanctions or trade embargoes.

CBP is the last line of defense in the export control process, as CBP can execute its border search authority, has the authority to enforce export control regulations, is physically located at the borders at our Nation's ports of entry, and has the ability to inspect, search, detain and seize goods being exported illegally or without the proper authorizations (licenses or license exemptions).

However, CBP is not alone in this endeavor. To combat the illegal export of U.S.-origin arms and other commodities, ICE also leverages multiple resources and their broad authorities in the areas of illegal export of munitions and sensitive dual-use technology, including sanction violations. Additionally, my colleagues at ICE inform me that in Fiscal Years 2006 and 2007, ICE's Counter-Proliferation Investigations (CPI) agents initiated more than 2,700 investigations into the illegal export of U.S. munitions and sensitive technology. These investigations resulted in 326 arrests, 326 indictments, and 237 convictions, which is more than any other US federal law enforcement agency.

The key to effective export controls is the collection and screening of export transaction information prior to the departure of cargo from the U.S. The Automated Export System (AES), was first deployed by the U.S. Customs Service, with the assistance of the U.S. Census Bureau, in 1995 to collect export transaction information for statistical and enforcement purposes. AES continues to be a key tool for CBP. The departments of Commerce and Homeland Security have worked diligently to author a Final Rule, which would revise part 30 of title 30 of the Code of Federal Regulations, Foreign Trade Statistics Regulations (15 C.F.R. Part 30), to implement mandatory AES filing of shipper's export declarations (SED). This Final Rule will assist CBP by strengthening our export enforcement capabilities. It is important that both the departments of Commerce and Homeland Security work together on an equal footing to enact future changes to these regulations to help meet our nation's security objectives. This Final Rule should be published in the near future.

CBP's ability to effectively screen exports using our risk management approach is dependent on receiving electronic information in advance of the departure of the cargo from the United States. The Trade Act of 2002 requires the Secretary of DHS to promulgate regulations mandating the electronic transmission of information pertaining to cargo to be exported from the United States prior to its export. The cargo information required to be transmitted is that information determined to be reasonably necessary to ensure cargo safety and security pursuant to the laws enforced and administered by CBP. The Act further indicates that the Secretary of DHS shall provide to appropriate Federal departments and agencies the cargo information it collects and, where practicable, implement regulations without imposing redundant requirements. CBP has published these regulations in addition to other export requirements, to include those pertaining to outbound manifests. To adequately assess and identify potentially high-risk shipments intended for export, it is essential to our enforcement efforts that advanced electronic information is provided through the AES for all shipments that require an SED. This will allow CBP sufficient time to screen high-risk cargo, while not impeding the movement of legitimate shipments leaving the United States.

CBP's long-term objective is to fully integrate U.S. exports into the International Trade Data Systems (ITDS) initiative. ITDS is an information technology initiative that aims to provide a single window for the international trading community to provide data to the Government for import and export transactions. CBP is the lead agency for the integration of participating government agencies under the ITDS umbrella, and the ultimate goal is full interoperability of all automated systems relative to exchanging and sharing transaction data.

Another aspect of CBP's export control operations is the use of the outbound cargo targeting module of the Automated Targeting System (ATS-Outbound) to assist in identifying and targeting exports which pose a high risk of containing goods that

may require export licenses, exports with potential aviation safety and security risks, such as hazardous materials, and shipments that are high-risk for export violations, such as smuggled currency, illegal narcotics, stolen property (including vehicles), U.S. munitions, sensitive U.S. technologies, or other contraband. ATS-Outbound extracts data from the SED that exporters file electronically through the AES. The data is sorted and compared to a set of rules and evaluated in a comprehensive fashion to assign a level of risk to the transaction.

If there is a question as to whether an export requires a license, CBP officers refer the shipment to the Exodus Command Center, which is managed by ICE. The Exodus Command Center is the principal administrative and operational technical center than coordinates with external export regulatory agencies to seek clarification or rulings in support of DHS export enforcement investigations. Specifically, the Exodus Command Center is the single point of contact for ICE special agents and CBP officers in the field to obtain operations support from national export licensing authorities, including Department of State, Directorate of Defense Trade Controls; Department of Commerce, Bureau of Industry and Security; Department of Treasury, Office of Foreign Asset Controls; Department of Energy, Nuclear Regulatory Commission; Department of Defense, and others. In Fiscal Year 2007, over 2,300 referrals were processed by the Exodus Command Center, including license determinations, license history queries, and other related requests. Based on the outcome of the Exodus Command Center queries, CBP may seize or release and ICE may initiate a concurrent criminal investigation.

CBP believes that the key to implementing effective export controls is to achieve full interoperability between all participating government agencies within the current export licensing regime that governs controlled commodities, rather than imposing a new licensing regime that would require every exporter to obtain a license to export. CBP does not see a benefit to imposing further licensing requirements on individuals or entities for the sole purpose of allowing them to use AES, which will be mandatory for exports requiring an SED in the near future with the publication of the Final Rule, as outlined above. The proposed creation of a new licensing regime would place an unneeded burden on the exporting community, since currently anyone can register to use AES, or AESDirect, an Internet-based module of AES. Further, it could slow the flow of commerce and potentially strain CBP resources, if CBP were required to validate whether an exporter was licensed or not prior to clearing export cargo.

In addition, an issue arises with the proposed system as to what occurs with the information after an exporter attempts to file a SED to a prohibited country or entity. The simple act of blocking the filing is insufficient, as it does not alert authorities that a prohibited entity or an entity in a prohibited country is trying to illegally procure sensitive U.S. goods. Because of DHS's broad export enforcement authorities and the department's role in the administration of AES, information associated with the proposed blocks and warnings should be provided to DHS and the Department of Commerce concurrently. Since the potential violations association with the blocks and filers fall under both the Department of Commerce regulations and the International Traffic in Arms Regulations, for which DHS has primary jurisdiction, it would serve the common good that information be forwarded to both agencies. This would also alleviate the need to create additional mechanisms designed to disseminate information derived from the filters among the different enforcement agencies. These scenarios would likely bring to light attempted violations and viable investigative leads.

Further, in establishing violations of export control laws, the government must prove that the defendant was aware of the licensing requirement and chose to violate it. In cases where exporters are warned that their export may require a license, a record of this warning should be saved. This information could help provide the requisite knowledge to prove violations. However, a drawback to the proposed system could occur in scenarios where a defendant is on trial for export violations resulting from intentional inaccurate AES filings. Because the proposed system would warn individuals when commodities may require a license or when the shipment appears to be contrary to U.S. export laws, a conceivable defense may be created when AES fails to notify the defendant that the export is prohibited, which could potentially mitigate the defendant's legal liability. Measures should be taken to inform exporters that the filers are set-up to provide additional protections, but are not in fact a "catchall" to prevent illegal exportation and it must be stressed that the exporter must still utilize due-diligence in determining whether or not their export requires a license.

CBP's frontline officers and agents, working in coordination with ICE special agents, will continue to protect America from terrorist threats and executing our traditional enforcement missions in immigration, customs, and agriculture, while

balancing the need to facilitate legitimate trade and travel. These initiatives discussed today are only a portion of DHS's efforts to secure our homeland, and we will continue to provide our men and women on the frontlines with the necessary tools to assist them in protecting our Nation's borders.

Regarding H.R. 5828, the Department of Homeland Security and other concerned agencies are currently reviewing this bill and will provide detailed observations to your Committee at a later date.

I would like to thank Chairman Sherman, Ranking Member Royce, and the members of the Committee, for the opportunity to present this testimony today. I will be happy to respond to any questions that you may have at this time.

Mr. SHERMAN. Thank you. Mr. Smith or Mr. Poe, you can go with questions first.

Mr. POE. Thank you. I would like to zero in on exporting military equipment to foreign countries.

Recently it has been reported that ITT, there is a contract with the United States; was convicted and paid, or will pay a \$100 million penalty for shipping night vision gear to China, of all places, the most advanced equipment that is used in Iraq and Afghanistan. And there have been other examples of military equipment being traded on eBay. EBay won't sell used cosmetics, but you can buy body armor on eBay, and some of these other examples.

So I want, I would like your opinion on, this is just one example of the one example I have given you about ITT. What can be done, how can we be more proactive, so that corporations that deal with the United States and export hardware—and I think you know these are, you know, war profiteers for nothing else, to China—how we can deal with them more effectively?

When you pay a fine, of course the executives don't pay the fine. Their corporation pays the fine. Maybe if some of them were shipped off to Guantanamo Bay prison, maybe they wouldn't do this in the future. I mean, we are looking for a use for Guantanamo.

But Mr. Borman, Mr. Owen, I would just like your input on this very sensitive issue.

And one last comment. When I was in Iraq over Easter weekend, I even had some military soldiers, troops on the ground very concerned about their equipment, like night vision goggles, getting in the hands of the bad guys. So where do we go to keep this from happening any further?

Mr. BORMAN. Maybe, Mr. Poe, I will start. The specific occasion you mentioned of course dealt with items that are controlled for export by the State Department, so that is not directly in my purview. But I think the principles are the same.

It is a constant effort to make sure that U.S. companies, whether they are big, medium, or small, understand what their specific requirements are under the regulations, whether they are dual-use or munitions. We continue to use devices like AES to monitor what is going out.

Frankly, we also have a lot of contacts in industry, because often we get our best tips from industry. But it is really a matter of continuing to make sure the companies, one, understand what the requirements are; and two, when there are violations to have severe-enough penalties.

And for example, on the dual-use side, that is one of the reasons it is very important for us to have reauthorized legislation. Because right now on the dual-use side, the penalties are quite old and not

as high as they should be, frankly. And the State Department in the ITT case, I think had a very vigorous prosecution of that case, working with DHS and the Justice Department.

But I think it is primarily continually reaching out to U.S. industry and making sure they understand what the requirements are. And also making sure they understand what the consequences are for failure to comply. You know, it is an ongoing challenge.

Mr. POE. But in your opinion, what do you think about going behind the corporate veil and having executives go to jail, rather than just pay a little fine?

Mr. BORMAN. The laws always allow for penalties and jail time for individuals. Of course, the evidence has to support that, and you have to make the case in the District Court, but that authority already exists. Again, I think it is a matter of whether the evidence, you know, can sustain that in a prosecution.

Mr. POE. Mr. Owen?

Mr. OWEN. I would say from a U.S. Customs and Border Protection viewpoint, the key for us is to have that advance information as to what is leaving the country before the cargo departs. We have a current rule that has been finalized to require mandatory submission to our Automated Export System of every shipment that is leaving, but there are still certain exemptions: Certain value thresholds, certain options that have been allowed to exist for some time.

I think in order for our frontline officers to be most effective, they have to have that advance information as to what is leaving the country before it leaves, so that we, as the law enforcement agency, can target it, send our officers to look at those shipments, and determine if it is going where it should be going, to people that are allowed to have it.

With holes in the system now, where certain export information can be filed post-departure, it really doesn't help us to keep that from happening up until it has already left the country.

But that would be the main item for U.S. Customs and Border Protection, would be to include the mandatory submission of all export declarations before the cargo leaves the country.

Mr. POE. All right. Thank you, Mr. Owen. Thank you, Mr. Chairman.

Mr. SHERMAN. Thank you. Okay. The Foreign Relations Authorization Act of 2003 required the State Department, which you work with closely, to publish regulations mandating the use by all parties required to file export information.

It has been 6 years since Congress passed that bill. Now we have another bill that we are considering which reimposes the same requirement. Basically, when are we going to see regulations—I mean, don't tell me we have got to pass another law mandating it. We have already passed one law. When are we going to see regulations mandating the use of AES by all parties required to file?

Mr. OWEN. The Secretary of Homeland Security has signed the final rule for mandatory submission of AES. There are still again certain caveats, certain options that allow for post-export filing, that we have been working with Commerce and with Census to close those loopholes, as well. But that is a positive improvement.

Mr. SHERMAN. So are we there yet? Or are we just close to getting there?

Mr. OWEN. We are very close to getting there.

Mr. SHERMAN. After only 6 years. And they say Congress operates slowly.

How many people are currently in jail now for violating the laws we are talking about here today?

Mr. BORMAN. I don't think I can give you that number off the top of my head.

Mr. SHERMAN. Under 10?

Mr. BORMAN. One thing I can tell you is that—

Mr. SHERMAN. Was anybody sentenced to serious jail time in 2007?

Mr. BORMAN. We have had a number of arrests in 2007, cases that just our agents worked on, which is not to say—

Mr. SHERMAN. We have had arrests, but that is really not my question.

Mr. BORMAN. 23 arrests, and 16 convictions.

Mr. SHERMAN. 16 convictions, but—

Mr. BORMAN. For criminal violations.

Mr. SHERMAN. For criminal violations. But we don't know if anybody was actually sentenced to do any time.

Mr. BORMAN. Well, I think they probably were. Because if there is a conviction—

Mr. SHERMAN. Often you get a conviction by cutting a deal under which the person will do no jail time. So we have 16 convictions for the entire United States for all of last year.

Mr. BORMAN. No, no, no. Sorry. That is 16 convictions that our agents worked on, dual-use.

Mr. SHERMAN. Oh, okay.

Mr. BORMAN. So there is another universe of munitions convictions that undoubtedly are out there. I don't know what those specific numbers are.

Mr. SHERMAN. Okay. But we don't know whether any of those 16 were sentenced to serious jail time.

Mr. BORMAN. That is something we can find out and get back to you on.

Mr. SHERMAN. I would like you to furnish that for the record.

There is the problem of dangerous materials being transshipped from the UAE to Iran. Recently, we saw the signing of the memorandum of understanding regarding the shipment of radioactive materials, and we have been pushing the UAE to strengthen its own export controls.

What are the steps being taken to work with authorities in Dubai to address the problem of transshipment of sensitive technologies to Iran? And what are our benchmarks for success in working with the UAE on this? Mr. Borman.

Mr. BORMAN. Well, as you already noted, in August 2007 the UAE passed its own export control law, which was a very significant milestone. That had been many years in the making.

Mr. SHERMAN. That is a milestone. But in many countries, including our own, written laws are kind of ignored by those who are supposed to carry them out.

Mr. BORMAN. Well, it is clearly a significant step, which is—

Mr. SHERMAN. It is a first step.

Mr. BORMAN. They are now in the process, so that law is on the books. There were press reports that they have actually arrested an individual for violating that law. Another important step for them to take is to make sure that their control list, which their law governs, at least covers all the items on the four multilateral export control regimes. They have a control list that has most of those but not all of those. So that is certainly another significant benchmark for them to achieve.

Mr. SHERMAN. Are the ones that are not covered, ones that you could legitimately argue shouldn't be subject for controls? Is there some rationality to their exclusion of some items?

Mr. BORMAN. My understanding was they based that list on a previous list that Singapore used. Singapore, for some reason, did not have a full control list. They now have a full control list. So I think that is the rationale that I have heard for that.

Mr. SHERMAN. So if there was any thought in the process of excluding certain items, that was thinking done in Singapore that the Singaporeans have since abandoned.

Mr. BORMAN. Well, they have concluded now they should have all the regime items on their list.

Mr. SHERMAN. Customs and Border Protection is charged with inspecting actual exports, verifying that they have the proper licenses, detaining questionable shipments, and seizing illegal exports. Customs and Border Patrol relies on an Automated Targeting System to identify exports for actual inspection by an officer.

What percentage of items on the Commerce Control list and the U.S. munitions list are actually inspected before export?

Mr. OWEN. I don't have that number. I can tell you that with our outbound enforcement operations, we make about 8,000 seizures a year. That is for the full range of all sorts of outbound violations, from currency to stolen vehicles, as well as violations off of these different lists.

But I can take that back. I don't have the exact number specific to those two examples of smuggling.

Mr. SHERMAN. Well, the question here is what percentage of items are physically inspected, not how many are seized. So I think that—you gave me a very interesting answer to a question that was more interesting than the one I asked. And I hope that you will answer this question for the record.

Mr. OWEN. Absolutely.

Mr. BORMAN. Mr. Chairman, if I could add a little bit to that. Again, not directly to that.

Mr. SHERMAN. Yes.

Mr. BORMAN. But we have had a system in place for many years whereby every day we download to CBP licensing decisions we have made that day, so that the inspectors at the ports and borders have the up-to-date electronic information on what has actually been licensed. And that is one of the pieces they use when then they check the AES filings.

Now again, that doesn't answer your question directly, but you know, it indicates we do have a system in place for them to get at that.

Mr. SHERMAN. Now, have you gentlemen reviewed H.R. 5828? What comments do you have about it?

Mr. BORMAN. My comments focus on Section 305, which is the export control-related piece. And as I said in the testimony, we support the broad goals of it. I think there are some technical comments, that are detailed in my written testimony, that we can work with staff on.

I think the main piece to be focused on is to make sure that the proposed changes are actually really implementable in practice. For example, the idea that you can correlate harmonized tariff code numbers with export control classification numbers. That is a very difficult and complicated undertaking, because those numbers are really designed for entirely different purposes.

So mandating that in the statute, I think we really have to think that through carefully and see how that could be done.

Mr. SHERMAN. If you have numbers that are used for different purposes, we have got these computer things we have come up with, why is it difficult to cross-reference numbers?

Mr. BORMAN. We did a check on some samples for one commodity, for example night vision thermal-imaging devices. There are multiple harmonized tariff code numbers that go to different pieces of that.

So this would be an extremely complicated and probably costly undertaking to figure out whether you could really correlate those.

Mr. SHERMAN. When you talk about costly, are you talking about \$1 million? Are you talking about \$1 billion?

Mr. BORMAN. In the millions rather than the billions. At least in our bureau, millions is very significant.

Mr. SHERMAN. But I mean, the GAO report references a cost for the bill of roughly \$10 million, at least. Is that the range we are talking about here?

Mr. BORMAN. I think in that range, yes.

Mr. SHERMAN. So it is really up to Congress to determine whether that is a good investment of \$10 million.

So there are some drafting aspects of the bill that you would like to work with the authors on. Then there is one policy decision. Is it worth many millions of dollars to harmonize these numbering systems and develop a computer system that achieves these objectives?

Mr. Owen, do you have any comments about that?

Mr. OWEN. One of the main concerns for Customs and Border Protection is when Section 3 deals with the operational changes that are suggested for AES.

AES was built, the Automated Export System, was designed and created in 1995 jointly with Census, and that remains primarily within the CBP realm of operation. And what we have done is we have linked our outbound targeting that we perform through our Automated Targeting System to the AES system.

So the suggestion that perhaps AES should be moved to one department, whereas ATS would stay within CBP, we are concerned that the linkages would be broken, and we wouldn't have as effective of a targeting tool for our frontline officers that use these systems every day.

Mr. SHERMAN. So the bill would take one agency or office out from your bureau and move it somewhere else?

Mr. OWEN. It would take the Automated Export System out from operational control within CBP, over to the Department of Census. However, our linkages to our targeting system, the ATS system, ties right in with that.

So what we are concerned with is a disconnect between the two linked systems in two different departments.

Mr. SHERMAN. I can see your concern. I have been in Congress 12 years; I have never seen any department testify that any function should be moved to another department. Nor have I ever seen any committee of jurisdiction argue for House rules that would transfer some of that jurisdiction to another committee.

It is amazing how the right thing to do for America is always to at least keep all of one's agencies and jurisdictions, and not to see them diminished. We are all dedicated to that patriotic goal.

With that, let me turn to Mr. Royce for his questions.

Mr. ROYCE. Thank you. I will begin, Mr. Owen, by asking you, you testified that the Customs and Border Protection is making 2,402 arrests every day between ports of entry. And if you multiplied that out for a year, that would be over 365,000. That would be 876,000 apprehensions.

And so I don't think most Americans realize just how many apprehensions you do make a day. But the estimates I have seen indicate that there is a ratio of three to one people who get through that apprehension process because the Border Patrol is under-funded.

And I was going to ask you, what are the trend lines there? And has that number of apprehensions gone up? Or what does it portend? I would ask you your opinion, Mr. Owen, on that.

Mr. OWEN. CBP's Office of Border Patrol does patrol between the ports of entry, whereas the Office of Field Operations that I am involved with works at the actual ports of entry.

I am not clear on whether or not, what the ratios are or the trend lines, but that is some information that we can take back, discuss with our Office of Border Patrol, and provide you the specifics on that.

Mr. ROYCE. Well, whatever the trend lines, existing circumstances are great.

Mr. OWEN. It is a significant number, yes.

Mr. ROYCE. Let me ask Mr. Borman. You testified that BIS conducted 850 end-use checks in 80 countries last year. I was going to ask you about the results of that. You know, how many violations you uncovered, where those violations were—that would be interesting—what is the challenge of assuring that dual-use technology isn't misused.

For example, if you have got some specific examples that might be enlightening to the members of the committee, we would like to hear it, Mr. Borman.

Mr. BORMAN. We generally discuss specific results on those end-use checks in more of a closed setting, because that is a more specific way—

Mr. ROYCE. I see.

Mr. BORMAN [continuing]. A better way for an exchange of information. But I can tell you generally there certainly are some numbers that come out that result in any range of actions. You know, some of them come out favorable; some of them come out unfavorable.

Mr. ROYCE. How about telling us which countries are the problematic countries, if you were to list them?

Mr. BORMAN. Well, again, it is better to talk about that in a closed session. But certain transshipment countries are ones that always warrant a lot of checks. We have many criteria that we apply to decide where we should do the checks, and transshipment countries are of course countries that rate high on that matrix, in terms of where we should go to look and the kinds of things we find there.

Mr. ROYCE. Well, I think at some point it would be good for the public to know who the primary abusers are of the process. But if you want to do that privately, I guess we can.

Why don't we go on with the rest of the witnesses and their questions, then? Thank you.

Mr. SHERMAN. The gentleman from Arkansas is recognized.

Mr. BOOZMAN. Thank you, Mr. Chairman.

Mr. Borman, you tell me about H.R. 5228, you said that there is no standard list of items for which an exporter must seek a license? I mean, that seems like that puts the burden on the exporter.

Mr. BORMAN. Well, it really varies. So for example, a high-performance computer. Under our system, that may require a license to certain countries or certain end users in countries, but not require a license to other end users in other countries. So we try to have a very differentiated system, so that U.S. exporters can compete for legitimate civilian business, but also the government has a chance to review transactions that would be more problematic.

So that is why, that is why it is hard to say definitively for any particular item, does it need a license to absolutely every place. You have a lot of differentiation there. And that is why it would be difficult to replicate that in toto, even in an Automated Export System.

Mr. BOOZMAN. So is that difficult for the exporter to figure out?

Mr. BORMAN. Well, in regulations we try to be as clear as we can. And we do a lot of outreach, both around the country and through our Web site, to try to make sure that people who have those questions can have them answered. And of course, some of them are relatively easy. If an embargo country, Iran or Cuba, everything going there needs a license. But again, a country like the UK or Germany or Japan are differentiated.

Mr. BOOZMAN. Would H.R. 5228 help better prosecute those breaking U.S. export laws?

Mr. BORMAN. Well, certainly I think with the revisions that we would recommend, I think it would be very helpful, to both prevent and prosecute. You know, because a big piece of what we try to do is not only prosecute violators, but try to prevent violations in the first place. As has been eluded to already, once a technology or an item is out of the country, it is out of the country.

Mr. BOOZMAN. And you feel like, though, that things need to be changed to give you the better ability to—

Mr. BORMAN. Certainly that would—yes, it would enhance our ability. You know, as would the passage of a new Export Administration Act to give us the undercover authority and foreign investigative authority.

Mr. BOOZMAN. Thank you, Mr. Chairman.

Mr. SHERMAN. The gentleman from Colorado.

Mr. TANCREDO. No questions.

Mr. SHERMAN. Mr. Borman, it looks like you are getting off easy here today.

Without objection, statements from agencies not represented here will be made part of the record. These may include various offices within DHS, DOD, Treasury, Energy, State, Justice, and the independent agencies.

You gentlemen are directed to provide answers to the questions for the record, the various questions that were asked. And with that, let us move on to the next panel.

Mr. BORMAN. Thank you, Mr. Chairman.

Mr. OWEN. Thank you.

Mr. SHERMAN. Gentlemen, thank you very much for being here.

As the next panel steps forward, I will sing their praises. We are going to welcome Mark Menefee, an expert in export enforcement. He has worked as acting director and then director of the Office of Export Enforcement in the Bureau of Industry and Security from 1993 until he joined Baker and McKenzie in 2004.

We also have with us Peter Powell, chief executive officer of C. H. Powell Company, senior counselor at the National Customs Brokers and Forwarders Association of America. Previously, Mr. Powell served as president of that organization. He has been involved with U.S. Customs efforts to automate reporting of commodity and transport export data.

And finally, we will welcome Arthur Shulman, who serves as general counsel of the Wisconsin Project on Nuclear Arms Control. Mr. Shulman is testifying in place of Gary Mulholland, who had a last-minute medical emergency and was unable to attend these hearings. We wish him a speedy recovery.

The Wisconsin Project carries out research and public education designed to inhibit the spread of weapons of mass destruction. In this capacity, Mr. Shulman manages the project research and advocacy for effective export controls.

Let us hear from our first witness.

**STATEMENT OF MARK MENELEE, ESQ., COUNSEL, BAKER &
MCKENZIE**

Mr. MENELEE. Mr. Chairman, members of the subcommittee, thank you very much for this opportunity to present my views on H.R. 5828 today.

My name is Mark Menefee. I serve as counsel at the law firm Baker and McKenzie, where I have practiced law for 4 years. Prior to that I served for 11 years as the acting director and then director of the Office of Export Enforcement in the Bureau of Industry and Security at the U.S. Department of Commerce.

I would like to underscore that today I am appearing before you in my own personal capacity, and my views are my own.

I commend you for your interest in the issues addressed in H.R. 5828. I hope my experience in both the law enforcement and the private sectors might be useful to you as the subcommittee considers this bill.

This bill merits your attention because it would help protect U.S. national security. It would assist the honest exporters in complying with the law, and it would assist law enforcement in detecting and prosecuting the knowing and willful violators.

That would be a lot to accomplish, I realize. I would like to begin by providing for you some background information about this Automated Export System, or AES, which is the subject of the bill. And especially how AES fits into the broader export control system.

This information will be presented for you at a high-level perspective, with regulatory details omitted.

In today's export control system, generally speaking there are only two occasions when the exporter will communicate formally with the U.S. Government about a particular shipment: When the exporter applies for a license, and when the exporter submits an AES record at the time of shipment. Those are essentially the only two occasions where the government can learn specific information about an export, such as who the parties to the shipment are, where it is going, and what is being shipped.

In this dangerous and changing world, where we have geopolitical rivals, proliferators of weapons of mass destruction, and terrorists, having only two opportunities to learn about an export shipment isn't comforting. We need to make the most of these two opportunities.

And moreover, one opportunity, the license, actually depends on a decision that has to be made by the exporter to submit an application to the government in the first place. If no application is submitted, the government has no chance to review that transaction before it leaves.

That leaves the government with its last opportunity, the humble AES record. The AES record is an electronic equivalent of the old hard-copy form known as the Shipper's Export Declaration. And that is a form that the government has used for more than 65 years. And like the old SED, the AES record is used for both trade statistics and export control purposes.

Generally speaking, an AES record must be submitted with each export shipment that either requires a license or that has a value of greater than \$2500, per Schedule B number. AES records are used to describe export shipments totaling over \$1 trillion worth of goods each year, but only a tiny fraction of that trade, in terms of dollar value and in terms of the number of shipments, requires prior export licenses.

Now, much of the debate about export control policy during the past 30 years has focused on licensing issues. And rightly so, because of the importance that licensable items have for the U.S. national security and foreign policy.

But in today's world, where you have a huge volume of export shipments, only a small percentage of which require prior license,

the government's challenge is how best to get the bulk of U.S. trade into compliance efficiently and effectively, using AES.

As has been discussed in the first panel, in 2002, and as Chairman Sherman noted, the Congress emphasized in 2002 the importance of complying with AES, when you passed the Security Assistance Act. That authorized the imposition of criminal and civil penalties for filing false AES records, or failing to file required records. Unfortunately, 6 years later, the Executive Branch still has not issued the final regulations implementing the statute.

Now I would like to briefly discuss H.R. 5828. This bill is policy-neutral regarding export restrictions. It only serves to improve the administration and enforcement of whatever export restrictions the government policymakers choose to impose.

The bill would accomplish three goals, basically. First, it would sharpen the impact of export restrictions. AES would be programmed to block immediately all entries concerning the restricted party or destination, and automation would be used to reduce the leakage that currently occurs from exporters who are simply not aware of the new restriction.

Second, this bill would help the honest exporters prevent inadvertent violations. AES would be programmed to provide warning notices in two areas where exporters face high liability risks: Screening customers against the government's restricted party list, and classifying the goods to determine licensing requirements.

Third, the bill would improve the ability of law enforcement officers to use AES to detect suspicious transactions. And notably, the bill's licensing certification and training programs for using AES would improve the accuracy and the timeliness of the data that are input into AES.

In addition, by requiring AES to provide warning notices to the filers, the bill would enhance the government's ability to prosecute the bad actors. These are the people who would disregard warning signs posted in AES with their filings and subsequently export U.S. products illegally.

Now, this may come as a surprise to the subcommittee, but I have to say that in my experience, in both the law enforcement and the private sectors, I have come to realize and appreciate how much the export enforcement and the business communities have in common on compliance issues.

The vast majority of exporters that I have met and worked with, both in my government role and in the private sector, are law-abiding. They do not disagree with the need for export controls, especially after September 11, 2001. They simply want to know what the rules are, and they will do their best to comply.

Moreover, when good exporters are in compliance, they have succeeded in managing their own liability risks, and they have reduced costs.

Good exporters have no sympathy for bad exporters. Bad exporters represent a small percentage of the overall trade, but it is their bad deeds that result in the regulations that burden the law-abiding exporters.

Law enforcement officers understand these percentages. Actually, the law enforcement officers, in my experience, want as many exporters as possible to comply with the rules. This is because when

the national security is at stake, it is critical to prevent violations from occurring. You might be able to prosecute a violator successfully after the fact, and that is well and good. But the goods that—

Mr. SHERMAN. Mr. Menefee, we do have to limit the statements to 5 minutes.

Mr. MENEFE. I am sorry, okay.

Mr. SHERMAN. If you could just provide us two sentences of conclusion.

Mr. MENEFE. Certainly. The interests of good exporters and law enforcement converge in the following ways. When more exporters are in compliance, it enables the law enforcement community to shift their limited resources to focus on the truly bad actors; namely, the terrorists and the foreign weapons procurement specialists.

In summary, I think this bill could do for the government and the country three things: Improve the sanctions, help honest exporters avoid mistakes, and help law enforcement detect and prosecute the knowing and willful violations.

Thank you very much.

[The prepared statement of Mr. Menefee follows:]

PREPARED STATEMENT OF MARK MENEFE, ESQ., COUNSEL, BAKER & MCKENZIE

Chairman Berman and Ranking Member Ros-Lehtinen, thank you for inviting me to testify before your subcommittee.

I commend you for your interest in the issues raised in H.R. 5828, *The Securing Exports Through Coordination and Technology Act*.

I have practiced law in the area of export controls for four years and before that I served for eleven years as the director of the Office of Export Enforcement in the Bureau of Industry and Security at the U.S. Department of Commerce. I am here today in my personal capacity and the views expressed are my own. I hope that my experience in both the law enforcement and private sectors might be useful to you as the subcommittee considers this bill.

H.R. 5828 would help protect U.S. national security, assist the honest exporters in complying with the law, and assist law enforcement in detecting and prosecuting the knowing and willful violators. That would be a lot to accomplish. But it is possible when you consider how the Automated Export System, or "AES," fits into the broader export control system. With your permission, I will provide a high level discussion of these issues, with regulatory details omitted, to explain how this system works.

In today's export control system, generally speaking, there are only two occasions in which the exporter will communicate in writing with the U.S. Government about a particular shipment: (1) when the exporter applies for a license; and (2) when the exporter submits an AES record at the time of shipment. On these two occasions the Government can learn the details of a particular export, such as: who are the parties to the shipment; where is it going; and what goods are being shipped.

In this dangerous and changing world, where we have geopolitical rivals, proliferators of weapons of mass destruction, and terrorists, having only two formal opportunities to learn the details of export shipments is not very comforting. We need to make the most of these opportunities.

Moreover, one opportunity, the license, depends on a decision made by the exporter to submit an application to the Government. If no application is submitted, the Government has no chance to review the transaction.

That leaves the Government with one last opportunity, the humble AES record. The AES record is the electronic equivalent of the hard copy form known as the Shipper's Export Declaration, or "SED," which the Government has used for more than 65 years. Like the SED, the AES record is used for trade statistics and export control purposes. Both the Export Administration Regulations, which apply to dual use items, and the International Traffic in Arms Regulations, which apply to defense articles, use the AES record as an export control document.

An AES record must be submitted to the Government with each export shipment that either requires an export license or exceeds \$2,500 in value. AES records are used to describe export shipments totaling over one trillion dollars worth of goods

each year. But only a tiny fraction of that trade, in terms of dollar value and number of shipments, requires prior export licenses.

Much of the debate over export control policy during the past 30 years has focused on licensing issues, and rightly so, because of the importance licensable items have for U.S. national security and foreign policy. But where you have a huge volume of export shipments, only a small percentage of which require prior licenses, the Government's challenge is how best to get the bulk of U.S. trade into compliance, effectively and efficiently, using AES.

In 2002, the Congress emphasized the importance of complying with AES when you passed the Security Assistance Act, which authorized the imposition of criminal and civil penalties for filing false AES records or failing to file required records. Unfortunately, six years later the Executive Branch still has not issued final regulations implementing this statute.

Now I will briefly discuss H.R. 5828.

This bill is policy neutral regarding export restrictions. It would only serve to improve the administration and enforcement of whatever export restrictions the Government policy makers choose to impose.

The bill would accomplish three goals.

First, it would sharpen the impact of the Government's export restrictions. AES would be programmed to block all entries concerning the restricted party or destination and warn the AES filer that the intended party or destination was prohibited. This would help restrictions take effect immediately in the export trade, and it would reduce the leakage that often occurs due to exporters who are not aware of the publication of the restriction.

Second, the bill would help honest exporters avoid committing inadvertent violations. AES would be programmed to provide warning notices in two areas presenting high liability risks for exporters: (1) screening customers against the Government's Restricted Parties Lists (which total approximately 6,000 names); and (2) classifying goods to determine license requirements.

The screening function would block the AES filer from being able to enter the name of a restricted party and would refer the filer to the appropriate Restricted Party List for guidance.

The classification function would be more complicated. It would assist the AES filer by correlating, to the extent feasible, the Harmonized Tariff System, or "HTS" number with an export classification number. Exporters are familiar with the HTS numbers for their goods because HTS is used worldwide for duty, quota, and statistical purposes. The HTS and export classification systems are different, however, with the latter being much more fine-grained than the former. At a minimum, the classification function could alert the exporter that an item classified under a particular HTS number is, or might be, classified for export control purposes on a control list maintained by the Commerce or State Department.

The logic for these warnings and alerts is straightforward. They help divide the good and bad exporters. Good exporters will follow them. Bad exporters will not, which brings us to the next goal.

Third, this bill would improve the ability of law enforcement officers to use AES to detect suspicious transactions. Currently law enforcement officers can review large numbers of transactions by using a search engine in the AES database. This can be a very effective enforcement technique. But these efforts are undercut by the high percentage of inaccurate AES records being filed. It is the old database problem of "garbage in, garbage out." By establishing a licensing requirement for AES filers, as well as a "pay as you go" training fund, the bill would greatly improve the accuracy of data input into AES, thereby enabling law enforcement to do its job better.

Installing warnings and alerts in AES would also enhance the Government's ability to prosecute bad exporters. For example, AES would retain records showing that on a particular date and time an exporter attempted to enter information for one AES record and was notified that a party was restricted. If the exporter subsequently entered information for a second AES record for the same transaction, and that second record contained fraudulent information, such as an alias for the restricted party, these records could be used as evidence in an enforcement proceeding against the exporter.

It may come as a surprise to the subcommittee, but from my experience in both the law enforcement and private sectors I have come to appreciate how much export enforcement personnel and law abiding exporters have in common.

The vast majority of exporters I have met or worked with are law abiding. Moreover, they do not disagree with the need to strong export controls. This is especially so after September 11, 2001. The good exporters simply want to know what the rules are. Then they do their best to comply. When they are in compliance, good

exporters have succeeded in managing their liability risks and reducing costs. Moreover, good exporters have no sympathy for bad exporters. While bad exporters may represent only a small percentage of the business community, their bad deeds lead to the regulations that burden the law abiding exporters.

Export enforcement officers understand these percentages of good and bad exporters. Actually, export enforcement officers want as many exporters as possible to comply with the rules. This is because when the national security is at stake, it is imperative to prevent violations from occurring. You might be able to prosecute a violator successfully after the fact. But if the goods reached the prohibited destination, the damage to the national security has been done. And it cannot be undone.

Thus, the interests of good exporters and export enforcement converge in the following way. When more exporters are in compliance, this enables the enforcement agencies to shift their limited resources from dealing with people who make honest mistakes to taking on the agencies' highest challenge, namely, to detect and stop the truly bad actors, such as terrorists and foreign weapons procurement operatives.

In summary, H.R. 5828 would improve the Government's implementation of export restrictions. The bill would help the honest exporters avoid costly mistakes. And the bill would help law enforcement detect and prosecute the knowing and willful violators. As I mentioned earlier, that would be a lot to accomplish. But it can be done by making some programming changes to the humble Automated Export System, which touches almost all exports from the United States.

Thank you for this opportunity to testify before your subcommittee.

Mr. SHERMAN. Thank you. Mr. Powell.

STATEMENT OF MR. PETER H. POWELL, SR., SENIOR COUNSELOR, NATIONAL CUSTOMS BROKERS AND FORWARDERS ASSOCIATION OF AMERICA, INC.

Mr. POWELL. Mr. Chairman, members of the subcommittee, good morning. I am Peter H. Powell, senior counselor to the National Customs Brokers and Freight Forwarders Association of America, fondly known as NCBFAA. I am also a professional ocean freight forwarder, and Chief Executive Officer of C. H. Powell Company in Canton, Massachusetts.

It is an honor to testify before you today.

NCBFAA is pleased to offer its support to H.R. 5828. The legislation we believe strikes the correct balance between improving the enforcement of our nation's export control laws and facilitating the ability of the private sector to export their product overseas.

H.R. 5828 also recognizes the difference between small, medium, and large exporters, a factor very compelling to NCBFAA, an organization that prides itself on representing the interests of small business.

First, allow me to tell the committee about NCBFAA. We have over 800 individual companies from throughout the United States who facilitate the movement of exports and imports. In the export realm, think of us as travel agents for cargo. We work with the exporter to arrange transportation of American goods to foreign markets. We are required to ensure that information is filed with the relevant Federal agencies with jurisdiction over the exports.

Finding means for reporting export shipments to the government has been the Shipper's Export Declaration, which is now available to filers in an automated mode through the Automated Export System, AES. Through this electronic pipeline, data is then sent to the agencies that have jurisdiction.

In the near future, AES will be integrated into Customs' soon-to-be-completed Automated Commercial Environment, ACE, and will connect to all the agencies of jurisdiction through the International Trade Data System, ITDS. This will mean an exporter can

file export data electronically through a single window, with the data then routed simultaneously to all relevant agencies for approval and oversight.

On-the-ground enforcement instructions will then be issued to Customs at the port. This will make AES an invaluable tool, providing the opportunity for better, more accurate enforcement, and more efficient disposition of cargo. Yet it becomes all the more critical that the information going into AES is accurate, reliable, and timely.

H.R. 5828 is an important step in meeting these objectives. The legislation establishes the Automated Export System as the primary instrument for inputting Shipper's Export Declaration data, and delivering that information to the appropriate Federal agency.

Importantly, it changes a paradigm. Presently when information is keyed into AES, the system will accept any information filed at face value. It is then up to the Federal agencies to identify prohibited or restricted exports as they flow throughout our ports.

As trade increases dramatically, the task of intercepting 100 percent of the goods that violate export control or trade sanctions becomes impossible.

Instead, H.R. 5828 uses the power of automation by requiring AES to have the capability to alert the exporter about licensing requirements, and AES will refuse to process the entry if it involves restricted parties or countries subject to trade sanctions. This will be an important compliance tool for an exporter making an inadvertent or honest mistake. It means that the filer will have the necessary resources to process export applications with greater confidence that they meet the letter of the law.

Legislation also provides assurance to the government that the filers of AES data have the requisite skills, knowledge, and professionalism to merit this trust by requiring filers to be licensed. It may seem unusual for a professional association to embrace licensing for its members. This position becomes more plausible, in light of our years of experience working with the Bureau of Census.

NCBFAA has worked harmoniously in developing the AES system and providing educational benefits to its members.

Under the bill, Census will accelerate its efforts to educate filers and provide tutelage for those processing lawful exports. Furthermore, the licensure provisions are not unduly burdensome.

National Customs Brokers and Forwarders Association of America support H.R. 5828, and thank the subcommittee for so expeditiously holding this hearing. We also congratulate Congressman Don Manzullo and Congressman Adam Smith for sponsoring a bill that will greatly advance the nation's export control system.

Gentlemen, thank you.

[The prepared statement of Mr. Powell follows:]

PREPARED STATEMENT OF MR. PETER H. POWELL, SR., SENIOR COUNSELOR,
NATIONAL CUSTOMS BROKERS AND FORWARDERS ASSOCIATION OF AMERICA, INC.

Mr. Chairman, I am Peter H. Powell, Sr., Senior Counselor to the National Customs Brokers and Forwarders Association of America (NCBFAA). I am also a professional ocean freight forwarder and chief executive officer of C.H. Powell Company of Westwood, Massachusetts. It is an honor to testify before you today.

NCBFAA is pleased to offer its support to H.R. 5828, sponsored by Representatives Don Manzullo and Adam Smith. The legislation, we believe, strikes the correct balance between improving the enforcement of our nation's export control laws and

facilitating the ability of the private sector to export their product overseas. H.R. 5828 is also clearly cognizant of the differences between small, medium and large exporters, a factor very compelling to NCBFAA, an organization that prides itself on representing the interests of small business. We believe that H.R. 5828 will greatly enhance our interaction with agencies involved in the export process, as well as advancing the interests of our exporting clients.

First, allow me to tell the committee about NCBFAA. We are comprised of over 800 individual companies, from throughout the United States, who facilitate the movement of exports and imports to their marketplace. In the export realm, think of us as travel agents for cargo: we work with the exporter in arranging transportation of American goods to foreign markets. Forwarders manage the movement of exported products in the air, sea and land modes. We are required to ensure that information is filed with the relevant agencies of the federal government so that they can determine conformity with our export control laws and meet the data collection requirements of the federal government. NCBFAA members work on a daily basis with the Department of Commerce's Bureau of the Census and Bureau of Industry and Security (BIS), as well as the Department of Homeland Security's Bureau of Customs and Border Protection (CBP).

The primary means for reporting export shipments to the government has been the Shipper's Export Declaration, which is now available to filers in an automated mode, the Automated Export System (AES). Through this electronic pipeline, data is directed to Census, BIS, State, Defense, OFAC, and other regulatory agencies with jurisdiction over exports. Ultimately, direction is provided to CBP, which acts as the federal enforcement agency at America's borders.

In the near future, AES will be integrated into CBP's soon-to-be-completed Automated Commercial Environment (ACE) and connect to the agencies of jurisdiction through the International Trade Data System (ITDS). Thus, by filing electronically through a *single* window, export data will be routed simultaneously to all relevant agencies for approval and oversight, while on-the-ground enforcement instructions will subsequently be issued to Customs at the port. The opportunity for better, more accurate enforcement and disposition of cargo makes AES an invaluable tool to both the government and exporter alike. But, it becomes all the more critical that the information going into AES is accurate, reliable and timely.

H.R. 5828 is an important step in meeting these objectives. The legislation establishes the Automated Export System as the primary instrument for inputting Shipper's Export Declaration data and delivering that information to the appropriate federal agency.

Importantly, it changes a paradigm. Presently, when information is keyed into AES, the system will accept any information filed at face value. It is then the responsibility of federal enforcement personnel to identify prohibited or restricted exports as they flow through our ports. As trade increases dramatically, particularly now during an unprecedented high water mark for exports, the task of intercepting 100% of the goods that violate export control or trade sanctions becomes impossible.

H.R. 5828 requires AES to use the power of automation to assist in this task by refusing to process illegal exports. The bill requires federal agencies to incorporate laws and regulations into AES that will alert the exporter about licensing requirements and deny processing where restricted parties or countries subject to trade sanctions or embargo are involved. This will be an important compliance tool for an exporter making an inadvertent or honest mistake. It means that the filer, most often our member, will have the necessary additional resources to process export applications with greater confidence that they meet the letter of the law.

The legislation also provides assurance to the government that the filers of AES data have the requisite skills, knowledge and professionalism to merit this trust, by requiring filers to be licensed. Candidly, it may seem unusual for a professional association to embrace licensure for its members. This position becomes more plausible in light of our years of experience working with the Bureau of the Census. NCBFAA has worked harmoniously in developing the AES system and providing education benefits to our members.

Under the bill, Census will accelerate its efforts to educate filers and provide tutelage for those processing lawful exports. Furthermore, the licensure provisions are not unduly burdensome:

- each company must have a licensed individual responsible for supervision and control of those employees who file SED data with AES;
- loss of a license is protected by reasonable due process procedures;
- and, acquisition of a license by a U.S. citizen or permanent resident is within the reach of those who meet qualification requirements reasonably expected of a responsible filer.

Our Education Foundation will develop the curriculum to educate our members in order to qualify for a license and then to meet Census' continuing education requirements. For those who are not members of our association, Census has authority under the bill to conduct similar such training for those seeking a license. In sum, Mr. Chairman, we are confident in the ability of professional freight forwarders to respond to this responsibility.

The National Customs Brokers and Forwarders Association of America support H.R. 5828 and thank the subcommittee for so expeditiously holding this hearing. We also congratulate Congressman Don Manzullo and Congressman Adam Smith for authoring a bill that will greatly advance the nation's export control system. The bill employs the power of automation both to improve enforcement and to make those requirements easier to negotiate for the exporting public. We thank you for this opportunity to speak on the bill's behalf.

Mr. SHERMAN. Thank you. Mr. Shulman.

**STATEMENT OF ARTHUR SHULMAN, ESQ., GENERAL COUNSEL,
WISCONSIN PROJECT ON NUCLEAR ARMS CONTROL**

Mr. SHULMAN. Thank you, Mr. Chairman. I am grateful for the opportunity to appear today before the distinguished members of the subcommittee, and to present my organization's views on the importance of strong export controls in stemming the spread of mass destruction weapons. I will be summarizing my written statement.

I will cover four topics. First, the dangers posed by the administration's present effort to weaken the export licensing process. Second, the need to improve industry's ability to police itself, including by strengthening the AES system. Third, the difficulties that will be created for verification and enforcement as the government continues to reduce licensing requirements. And fourth, the risks of transshipment and diversion posed by places like Dubai.

I believe that the basic point is simple. If our Government continues to diminish export controls, we will pay the penalty of watching our own products arm our enemies. The risks are real, and the consequences of ignoring them are also real, as we are now learning in the financial arena.

The same is true for national security. There are a number of ways in which the administration has chosen to reduce controls. There is the Validated End User Program, VEU, initiated last year by the Commerce Department. That program allows select companies to receive controlled dual-use goods without export licenses.

Then there are the Defense Trade Cooperation Treaties with the United Kingdom and Australia, now awaiting approval by the Senate. These treaties would create new communities of buyers in those two countries, who could receive munitions items from the United States license-free.

Both the VEU program and the treaties depend on identifying trusted customers abroad. Yet it is far from clear whether the government agencies seeking to rely on such trusted buyers are able and willing to screen carefully, and to verify sufficiently.

In January, my organization published a report on the VEU program. We found that two of the first five Chinese VEUs, hand-picked by Commerce, are linked to China's military industrial complex, to Chinese proliferators sanctioned by the United States, and to U.S. companies accused of export violations.

Part of the problem is that the program's procedures are not well-defined, and appear to be getting weaker. The BIS has already

abandoned mandatory verification visits and annual reporting requirements. Commerce touts the already large volume of exports to China that are freed from licenses under the VEU program.

Congress should insist that the program be halted until the Government Accountability Office determines that it does not reduce our national security.

The defense trade cooperation treaties with the UK and Australia may be heading down the same dangerous path. The treaties establish new exemptions from export license requirements for arms trade with those countries. The treaties and their implementing arrangements leave many questions unanswered about which companies will be deemed trusted, and how our Government will ensure that they continue to be trustworthy.

Both the VEU program and the treaty exemptions serve to decrease our Government's role in controlling sensitive exports. This creeping abrogation of a key national security function is highly risky. By eliminating the pre-shipment checks performed by licensing officers, responsibility for spotting and preventing diversion attempts shifts to the exporter, who may lack the necessary training and resources, and to Customs officials, who may lack the ability to screen license-free exports adequately before they leave U.S. ports.

Greater reliance is being placed on industry to screen its own transactions, without enough guidance from the government. An example is the Entity List maintained by BIS, by Commerce. The list is supposed to be a primary means for informing exporters about foreign entities that pose a risk of diversion, triggering a license requirement. But the list is incomplete and out of date. One entry tries to warn about a Chinese factory posing a risk of diversion to missile end-uses. But it doesn't provide enough information to identify the factory.

After trying for years to convince BIS that the Entity List must be updated and made more useful, we decided to do the work ourselves. In April we posted on our Web site an annotated version of the Entity List's China section, complete with updated entity names, including in Chinese, and contact information. We invite industry to use this new resource for more effective export screening. And we also hope that BIS will incorporate our updates in the official Entity List, and make additional requested changes. Then the Entity List can become a real tool for industry to screen its exports, and to prevent diversions.

Mr. Menefee and Mr. Powell have outlined how the Automated Export System can be made stronger, and the role that it can play both to help industry screen its exports, and to help export control officials to carry out their duties under the law.

H.R. 5828 contains some very good ideas for helping exporters and export control officials. The bill would make classification decisions for exporters, and would screen their transactions against the restricted party lists. These services are now available commercially, but are not affordable for all.

We believe that H.R. 5828 could go further to make AES what it must become, in light of the trend toward reduced licensing.

My prepared statement includes some additional suggestions for improving the bill. These changes would make AES more com-

prehensive and more useful, both for industry and for export control officials.

Indeed, the Automated Export System must become more robust, since in absence of export licenses, it may be the only record the U.S. Government has of exports under “trusted customer” programs.


The GAO, Customs, and the Justice Department have all noted evidentiary and other concerns about investigating and prosecuting violations when licenses are not required. And the House International Relations Committee has noted that export violations are less likely to be prosecuted and penalized in such cases.

I would also like to thank Chairman Sherman for highlighting the risks of transshipment and diversion via Dubai today.

I would like to offer for inclusion in the record an article listing transshipments of dangerous items through Dubai and elsewhere in the United Arab Emirates. The article was authored by my organization—

Mr. SHERMAN. Without objection, so ordered.

[The information referred to follows:]



[about us](#) | [our achievements](#) | [contact us](#)

Home

Publications **Nukes 'R' Us**

Country Info By Gary Milhollin and Kelly Motz

Export Controls *The New York Times*

Risk Report March 4, 2004, p. A31

Iran Watch WASHINGTON - America's relations with Pakistan and several other Asian countries have been rocked by the discovery of the vast smuggling network run by the Pakistani nuclear scientist Abdul Qadeer Khan. Unfortunately, one American ally at the heart of the scandal, Dubai in the United Arab Emirates, seems to be escaping punishment despite its role as the key transfer point in Dr. Khan's atomic bazaar.

Iraq Watch

About Us

Iran's weapon progress Dubai's involvement is no surprise to those who follow the murky world of nuclear technology sales. For the last two decades it, along with other points in the emirates, has been the main hub through which traffickers have routed their illegal commerce to hide their trails. Yet the United States, which has depended on the emirates as a pillar of relative stability in the Middle East and, since 1991, as a host to American troops, has done little to pressure it to crack down on illicit arms trade.

A status report from IranWatch on Iran's ability to produce mass destruction weapons.

[Read the Update](#)

Receive Wisconsin Project news and updates by e-mail.

[Sign up today](#)

American authorities say that Mr. Tahir also bought centrifuge parts in Europe that were sent to Libya via Dubai. In return for millions of dollars paid to Dr. Khan, Libya's leader, Col. Muammar Qaddafi, was to get enough centrifuges to make about 10 nuclear weapons a year.

Why ship through Dubai? Because it may be the easiest place in the world to mask the real destination of cargo. Consider how the Malaysian government is making the case for the innocence of its manufacturing company. "No document was traced that proved" the company "delivered or exported the said components to Libya," according to the country's inspector general of police. The real destination, he said, "was outside the knowledge" of the producer. One can be certain that if the Khan ring's European suppliers are ever tracked down, they will offer a similar explanation.

Dubai provides companies and governments a vital asset: automatic deniability. Its customs agency even brags that its policy on re-exporting "enables traders to transit their shipments through Dubai without any hassles." Next to Dubai's main port is the Jebel Ali free trade zone, a haven for freewheeling international companies. Our organization has documented 264 firms from Iran and 44 from rogue regimes like Syria and North Korea.

With the laxity of the emirates' laws, there is simply no way to know how many weapon components have passed through. But consider some incidents that our organization has tallied - based on shipping records, government investigations, court documents, intelligence reports and other sources - over the last 20 years.

. In 1982, a German exporter and former Nazi, Alfred Hempel, sent 70 tons of heavy water, a component for nuclear reactors, from Sinochem in China to Dubai. The shipping labels were then changed to mask the transaction, and 60 tons of the heavy water were forwarded to India, where it enabled the government to use its energy-producing reactors to create plutonium for its atomic weapons program. The other 10 tons went to Argentina, which was interested in atomic weapons at the time.

. In 1983, Mr. Hempel sent 15 tons of heavy water from Norway's Norsk Hydro, and 6.7 tons from Techsnabexport in the Soviet Union, through the emirates to India.

. In 1985 and 1986, Mr. Hempel sent 12 more tons of Soviet heavy water to India that were used to start the Dhruva reactor, devoted to making plutonium for atomic bombs. (The details of these transactions come from German and Norwegian government audits, but Mr. Hempel, who died in 1989, was never convicted of a crime.)

. In 1990, a Greek intermediary offered Iraq an atomic-bomb design (probably of Chinese origin) from Dr. Khan in Pakistan, with a guarantee that "any requirements or materials" could be bought from Western countries and routed through Dubai. Iraq has said it rejected the offer and suspected it of being part of a sting operation, although a more likely explanation is that the impending 1991 Persian Gulf war precluded the deal.

. In 1994 and 1995, two containers of gas centrifuge parts from Dr. Khan's labs were shipped through Dubai to Iran for about \$3 million worth of U.A.E. currency.

. In 1996, Guide Oil of Dubai ordered American-made impregnated alumina, which can be used for making nerve gas ingredients, and tried to pass it along to an Iranian purchasing agent, Drush Jamshidnezhad, in violation of American export control laws. A sample was delivered before the deal foundered when middlemen were caught by American officials in a sting operation.

. Also in 1996, the German government listed six firms in Dubai as front companies for Iranian efforts to import arms and nuclear technology.

. From 1998 to 2001, several consignments of rocket fuel ingredients shipped to Dubai by an Indian company, NEC Engineers, were sent to Iraq, in violation of Indian law and the United Nations embargo on Saddam Hussein's regime.

. In 2003, over Washington's protests, emirates customs officials allowed 66 American high-speed electrical switches, which are ideal for detonating nuclear weapons, to be sent to a Pakistani businessman with longstanding ties to the Pakistani military. American prosecutors have indicted an Israeli, Asher Kami, for allegedly exporting the switches through Giza Technologies in New Jersey to South Africa and then to Dubai.

The pattern is terrifying, and those examples are most likely a small part of the overall picture. So, will the Bush administration, with its focus on fighting terrorism and the spread of weapons of mass destruction, start cracking down on the emirates? The first signs are not promising. President Bush has warned of interrogations in Pakistan and actions against the factory in Malaysia that supplied Dr. Khan, but has given no hint of any penalties against Dubai. Lockheed Martin is about to send 80 F-16 fighters to the emirates, and a missile-defense deal may be in the offing.

The lesson of the Khan affair is that instead of focusing solely on "rogue regimes," we have to shut down the companies and individuals that supply them with illicit arms and technology. The United States and its allies have to put pressure on the countries that allow the trade to flourish - even if it means withholding aid and refusing arms sales. Unless Dubai cleans up its act, it should be treated like the smugglers it harbors.

Gary Milhollin is director of the Wisconsin Project on Nuclear Arms Control. Kelly Motz is associate director.

Copyright © 2003 - 2008
Wisconsin Project on Nuclear Arms Control
1701 K Street, NW, Suite 805 Washington, DC 20006
tel: 202-223-8299 fax: 202-223-8298

[The Risk Report](#) - [Iran Watch](#) - [Iraq Watch](#)

[about us](#) | [our achievements](#) | [contact us](#)

Mr. SHULMAN. Thank you. It appeared in the New York Times on March 4, 2004. Unfortunately, as Mr. Sherman pointed out, things have not improved much since then. Dual-use goods, including specialized metals, aircraft parts, and gas detectors apparently have continued to move through Dubai to Iran, Syria, and Pakistan.

I would like to highlight the case of Mayrow General Trading in Dubai, where American-made computer circuits were received by this company, thereafter diverted to Iran, and eventually turned up in unexploded roadside bombs in Iraq.

In what was widely viewed as a public threat to the Emirates, the Commerce Department proposed, in February 2007, to designate "destinations of diversion concern," and to impose additional restrictions on exports to such places. However, that proposal stalled after UAE officials promised to adopt an export control law. Emirates officials point to a handful of enforcement actions since the law was adopted last year.

But even Dubai traders red-flagged by the United States say that little has actually changed. Dubai is still a great security risk, as Iran continues to import large quantities of goods through its revolving door. It will not be possible to curb Iran's nuclear imports unless Dubai and the UAE clean up their act.

My organization supported the "destinations of diversion concern" proposal when it was issued, and recommended that the UAE be so designated immediately. We recommend now that Congress take this step through legislation. Such a designation would send a strong public signal that there are consequences for choosing profit over international security. The UAE should be treated the same way for export control purposes as countries like Pakistan, that are using it as a diversion point.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Shulman follows:]

PREPARED STATEMENT OF ARTHUR SHULMAN, ESQ., GENERAL COUNSEL, WISCONSIN
PROJECT ON NUCLEAR ARMS CONTROL

I am pleased to appear before this distinguished Subcommittee to discuss the importance of strong export controls in stemming the spread of mass destruction weapons.

I will cover four topics. First, the dangers posed by the administration's present effort to weaken the export licensing process; second, the need to improve industry's ability to police itself; third, the difficulties that will be created for verification and enforcement as the government continues to reduce licensing requirements; and fourth, the risks of transshipment and diversion posed by places like Dubai.

A nuclear sub-prime crisis?

For over a decade, we have seen a consistent push by industry to weaken U.S. controls on the export of militarily sensitive technologies. Though tasked with protecting U.S. national security, successive administrations have succumbed to the pressure to "modernize" export controls and to make them less "burdensome" and more "efficient." The result has been to emphasize greater profits from exports and disregard the risk that American products will be diverted. This policy is very like the one that some of our banks adopted recently when they disregarded risk, thought only of profits, and shoveled money out the door to finance real estate sales. Risks are real, and the penalties for ignoring them are real, as we are now learning in the financial arena. The same is true for national security. If our government continues to diminish export controls, we will pay the penalty of watching our own products arm our enemies. We will have produced the equivalent of a nuclear sub-prime crisis.

There are a number of ways in which the administration has chosen to reduce controls. I will discuss two of them here today. First, there is the “Validated End-User” (VEU) program initiated last year by the Commerce Department. That program allows select companies to receive controlled dual-use goods without export licenses. Second, there are the defense trade cooperation treaties with the United Kingdom and Australia, now awaiting approval by the Senate. These treaties would create new “communities” of buyers in those two countries who could receive munitions items from the United States license-free.

Making sure the “trusted” are trustworthy

Both the VEU program and the treaties depend on identifying “trusted” customers abroad. Yet, it is far from clear whether the government agencies seeking to rely on such “trusted” buyers are able and willing to screen carefully and to verify sufficiently. In January, my organization published a report on the VEU program. The report revealed that the “trusted” customers being chosen were not necessarily trustworthy.

The Commerce Department’s Bureau of Industry and Security (BIS) claims to select each Validated End-User based on “the entity’s record of exclusive engagement in civil end-use activities,” and on “the entity’s relationships with U.S. and foreign companies,” among other factors. BIS also requires VEU applicants to supply an “overview of any business activity or corporate relationship that the entity has with either government or military organizations.” All of this information is supposed to be vetted by BIS and by an interagency committee, which must approve each candidate unanimously. But our report on the program reveals that two of the first five Chinese companies designated as VEUs are closely linked to China’s military-industrial complex, to Chinese proliferators sanctioned by the United States, and to U.S. companies accused of export violations. Commerce hand-picked these companies, tellingly noting that they accounted for 18% of licensed U.S. exports to China.

Part of the problem is that Commerce’s procedures are not well-defined and appear to be getting weaker. For example, BIS intended to rely on mandatory end-use visits in China to verify that American exports were not being diverted. But the Chinese Ministry of Commerce refused blanket consent to such visits. BIS then settled for reviews if “warranted” and with ample notification to the Chinese government. BIS has also eliminated a requirement that U.S. exporters report annually what they sell under the VEU program. BIS argued that it can already access this information through the Automated Export System (AES), despite questions as to whether the system can track this data in the detail required. Congress should insist that the program be halted until the GAO determines that it does not reduce our national security.

The defense trade cooperation treaties with the United Kingdom and Australia are heading down the same dangerous path. The treaties establish new exemptions from export license requirements for arms trade with each of those countries. But the treaties, as well as their implementing arrangements, leave many important questions unanswered.

The treaties allow license-free arms exports to foreign buyers in “approved communities” and for an as-yet undisclosed list of “operations, programs and projects.” But as with the VEU program, details are unclear about which companies will be deemed “trusted,” and how our government will ensure that they continue to be trustworthy. For example, it is unclear whether the government will screen freight forwarders and other intermediaries involved in arms sales under the treaties. The treaties and their implementing arrangements are also vague about verification, site visits and inspections.

Both the VEU program and the treaty exemptions serve to decrease our government’s role in controlling sensitive exports. This creeping abrogation of a key national security function is highly risky. By eliminating the pre-shipment checks performed by licensing officers, the responsibility for spotting and preventing diversion attempts shifts to the exporter—who may lack the necessary training and resources—and to customs officials, who may lack the ability to screen license-free exports adequately before they leave U.S. ports.

Greater reliance on industry—with little help from government

Although greater reliance is being placed on industry to screen its own transactions, industry has never received enough guidance from the government. An example is the Entity List maintained by BIS. The List is supposed to be a primary means for informing exporters about foreign entities that pose a risk of diversion. An exporter usually must apply to BIS for a license before selling to an entity on the List. The List, however, is incomplete and out of date, especially its China section. For example, an organization listed seven years ago as “13 Institute, China

Academy of Launch Vehicle Technology, (CALT), a.k.a. 713 Institute or Beijing Institute of Control Devices” is no longer part of CALT. It is now subordinate to the China Aerospace Times Electronics Corporation (CATEC). Another entry is a mystery: “Xiangdong Machinery Factory.” There are several entities in China with current or former names that can be translated in full or in part as “Xiangdong Machinery Factory,” yet the List supplies no other identifying information about the entity it means to designate.

The Entity List is wholly insufficient to help exporters identify the risky companies and organizations of which they should be wary. Despite criticism from auditors and requests from industry and national security advocates, little has been done to ensure the currency and usefulness of information now on the List.

For several years, the Wisconsin Project has tried through various channels to convince BIS that the Entity List must be updated and made more useful. This spring, we grew tired of waiting and decided to do the work ourselves. In April, we posted on our website (at www.wisconsinproject.org) an annotated version of the Entity List’s China section, complete with updated entity names (including in Chinese) and contact information. We invite exporters to use this new resource for more effective export screening. We also hope that BIS will incorporate our updates in the official Entity List, and make additional requested changes. Then the Entity List can become a real tool for exporters to screen their exports and prevent diversions.

Revising the Automated Export System: H.R. 5828

The automated export compliance screening proposed for the Automated Export System (AES) by H.R. 5828 also has great potential for helping exporters. It would make classification decisions for exporters, and would screen their transactions against the restricted party lists. Such services are now available commercially, but are not affordable for some exporters.

Although H.R. 5828 contains sound ideas, it does not go far enough to make AES what it must become in light of the current trend toward reduced licensing. The following changes would improve the bill:

- AES should provide comprehensive coverage of export information. The bill, however, allows the Secretary of Commerce to grant exceptions to mandatory *a priori* filing. To keep such exceptions to a minimum, they should require interagency approval.
- AES must be kept abreast of export control laws and regulations, and it must gather complete information for blocking, tracking and enforcement purposes. AES was not ready to perform a key function for the VEU program (identifying the exported item fully) at the time of VEU implementation; this should not happen.
- Sharing of AES data with other appropriate federal agencies should be mandatory, and procedures for such sharing should be transparent. For example, members of the interagency committee charged with selecting Validated End-Users should be able to track VEU exports independently to verify that each “trusted” customer remains trustworthy. Federal investigators and prosecutors should have ready independent access to export data.
- In the proposed scheme to license AES filers, procedures for revocation or suspension of licenses should include an option to suspend a license immediately (blocking access to the system) if a violation of export control or AES rules is imminent. An analogy is the Temporary Denial Order available under the Export Administration Regulations.
- The automated export control screening/blocking mechanism for AES could reduce inadvertent errors by filers and help less experienced exporters. By retaining filing data, the system could also decrease diversion risk by limiting bad actors’ ability to “game” the system without being discovered.
 - Automated screening should be comprehensive across the AES system. It should encompass all export control regulations relevant to AES (including those of the Nuclear Regulatory Commission) and should screen against all restricted party lists (including administrative debarments under ITAR part 128).
 - The bill does not explain how the automated screening model would apply to the exporters who use post-shipment filing. If post-shipment filing is to continue, its “trusted” users must be vetted even more thoroughly.
 - The system should be more consistent in screening transactions. The bill describes export compliance conditions which should generate a “fatal error” for an AES filing attempt, and other conditions which merit only “warning” messages. But some of the conditions resulting in warnings

do not appear to be qualitatively different from those producing “fatal errors.”

- The bill should explicitly mandate the recording and retention of AES users’ actions while filing export data, and should allow for use of such data for enforcement. This would allow detection of attempts to circumvent controls by changing information initially rejected by the screening system.

Verification and enforcement are more difficult without export licenses

The GAO has noted concerns from the Justice Department and from Customs about investigating and prosecuting violations when exemptions from licensing requirements apply. The GAO found that “it is particularly difficult to obtain evidence of criminal intent since the government does not have license applications and related documents that can be used as proof that the violation was committed intentionally.” In addition, the Justice Department itself has pointed to the importance of the “domestic evidentiary trail” created by the licensing process, and warned that licensing exemptions for countries (like those created by the munitions treaties) could “greatly impede the ability of the law enforcement community to detect, prevent and prosecute criminal violations.” In the absence of export licenses, it appears that the Automated Export System will be the only record the U.S. government has of exports under “trusted” customer programs. Further, the House International Relations Committee has noted the inclination of the courts to “view the licensing requirement as highly relevant to the establishment of a person’s legal duty under U.S. law” and the tendency of federal prosecutors to “regard the absence of a license requirement as signifying an activity of lesser importance to the U.S. government . . .”

As fewer exports of sensitive goods are screened by licensing officials, export control must also rely more on Customs to review outgoing shipments and verify the self-policing activities of industry. But there is evidence that Customs may not be up to the task. Customs and Border Protection (CBP) of the Department of Homeland Security (DHS) is charged with inspecting outbound shipments. But in September 2007, the DHS Inspector General reported that “outbound shipments are not consistently targeted and inspected by CBP Officers at the ports for compliance with federal export laws and regulations . . . because CBP does not devote sufficient resources to the function [and] does not have the information necessary to effectively monitor the program.” Immigration and Customs Enforcement (ICE), also at DHS, is responsible for investigating export violations. But ICE is also responsible for immigration enforcement. The rapidly growing demands of this competing function may well diminish the resources available for export control.

Oversight remains necessary

Until last year, the Inspectors General of the Departments of Commerce, Defense, Energy, and State, in consultation with the Director of Central Intelligence and the Director of the Federal Bureau of Investigation, were required by statute to assess whether export controls and counterintelligence measures are adequate for preventing the acquisition of sensitive U.S. technology and technical information by countries and entities of concern. The Inspector General at the Department of Homeland Security also participated in these reviews. The Inspectors General identified numerous shortcomings, prompting improvements. These reviews should be re-instituted and made permanent.

Transshipment and Diversion—the case of the United Arab Emirates

The subcommittee has asked me to discuss the risks of transshipment and diversion. I would like to offer for inclusion in the record an article listing transshipments of dangerous items through Dubai in the United Arab Emirates. The article appeared in the *New York Times* on March 4, 2004. Unfortunately, things have not improved much since then.

My organization has documented how Dubai and other points in the United Arab Emirates have served for decades as the main hubs in the world for nuclear and other smuggling. In the 1980’s, several shipments of heavy water, a nuclear reactor component, were smuggled from China, Norway and the Soviet Union through Dubai to India, so India could use its reactors to create plutonium for nuclear weapons. In the 1990’s, companies in Dubai willingly coordinated the notorious smuggling network of Pakistani scientist A. Q. Khan. Through Dubai to Iran were shipped two containers of gas centrifuge parts from Mr. Khan’s laboratories for about three million dollars worth of U.A.E. currency. Also in the 1990’s, a Dubai company attempted to violate U.S. export control laws by shipping Iran a material useful for manufacturing ingredients for nerve gas, and the German government listed six firms in Dubai as front companies for Iranian efforts to import arms and

nuclear technology. In October 2003, Emirates customs officials, over U.S. protests, allowed 66 high-speed electrical switches ideal for detonating nuclear weapons to be sent to a Pakistani businessman with ties to the Pakistani military. An affidavit, signed by an official in the U.S. Department of Commerce, shows that the director of customs in the Emirates refused to detain the shipment despite a specific request by one of the Department's agents.

Even more recently, American-made computer circuits received by Mayrow General Trading in Dubai were diverted to Iran, and eventually turned up in unexploded roadside bombs in Iraq. Other dual-use goods—including specialized metals, aircraft parts and gas detectors—have also continued to move through Dubai to Iran, Syria and Pakistan. Until the Mayrow discovery, the U.S. government had quietly pressed Emirates officials (with little success) to monitor U.S.-origin dual-use goods in the UAE, and to do more to prevent their diversion. After Mayrow, the administration issued what was widely viewed as a public threat to the Emirates. The Commerce Department proposed in February 2007 to designate “Destinations of Diversion Concern,” and to impose additional restrictions on exports to such places.

But the proposal stalled after UAE officials promised to adopt an export control law. The law was adopted last year, and Emirates officials point to a handful of enforcement actions since then. Nevertheless, export control experts and even Dubai traders red-flagged by the United States say that little has actually changed. Dubai is still a grave security risk. Iran continues to import large quantities of goods through Dubai's revolving door. It will not be possible to curb Iran's nuclear imports unless Dubai and the other Emirates clean up their act.

My organization supported the “Destinations of Diversion Concern” proposal when it was issued, and recommended that the United Arab Emirates be so designated immediately. I recommend now that Congress take this step through legislation. Such a designation would send a strong public signal that there are consequences for choosing profit over international security. The UAE should be treated the same way for export control purposes as countries like Pakistan that are using it as a diversion point.

Mr. SHERMAN. Thank you. I will recognize first for questioning, Mr. Boozman, if he has any questions. I am going to go last, as Mr. Wu needs to leave.

Mr. BOOZMAN. Thank you, Mr. Chairman. You mentioned the Chinese and Dubai. What other countries, Mr. Shulman, are at the top of the list as far as trying to procure things that they shouldn't be procuring?

Mr. SHULMAN. Well, Congressman, Dubai and the UAE are certainly the most notorious, and the most incorrigible in this respect. They are also the place that we have studied and analyzed the most.

China is certainly a concern, as our Government has pointed out again and again. I will be happy to provide you with a list of additional countries that should be scrutinized in this way.

Mr. BOOZMAN. You mentioned the components going through Dubai that wind up in roadside bombs. Were those components things that would be prohibited from being exported? In other words, you could have a timer, you know, is okay. But like I said, were those particular components, would they have attracted attention? Do you understand what I am saying, normally?

Mr. SHULMAN. Yes, sir, I do. They would certainly be prohibited from being exported to Iran, as Iran is subject to an embargo by the United States. And this is precisely why exports of dual-use goods to the UAE should receive special scrutiny, because of the likelihood of diversion.

Mr. BOOZMAN. Mr. Powell, the concerns that I have, and I think a lot of others, with any legislation when we are being more restrictive, is that we don't—most of these companies that are going to break the law are going to break it regardless of what we do,

to a large extent. Okay? In other words, they are going to find a way to go around the rules.

What we don't want to do is put onerous restrictions on those that are trying to do their best with, you know. I know that when we go in and close on a house, we sign a group of documents this large that nobody reads, okay.

So do you feel comfortable, representing the group that you represent, do you feel comfortable that this is not going to do that?

Mr. POWELL. Oh, I feel very definitely this is an aid and an assist. And it will prevent the inadvertent mistake.

Mr. BOOZMAN. Do you think it will actually help your membership?

Mr. POWELL. Oh, without question. And our membership or our industry probably represents 80 percent of the filers through AES. And therefore, to have access to various lists or so forth, or who you are doing business with as the end use and the end user that really become the most important.

And unfortunately, due to, you know, people within companies and so forth and so on, the education level does not reach the level that the U.S. would like to see. Therefore, having assists like this, extremely important. It won't prevent the bad guy necessarily, but it certainly will prevent those inadvertent errors.

Mr. BOOZMAN. Mr. Shulman testified that he would actually like to see this thing tightened up even more.

Mr. Menefee, do you see any way that we could improve the bill? Is there anything you would like to see? I know you are testifying for the bill. Is there anything that you would like to—you heard the testimony of the first group, who actually were supportive of doing something.

Mr. MENEFEE. Well, yes, sir. Thank you. I think there are two ways in which the bill could be strengthened. And that would be, number one, to require that if the U.S. Government is going to publish a sanction against a particular bad guy, an entity, an institute, or a trading company in Dubai, for that matter, they need to include the address. Because in a world of shipping products, the address matters a great deal.

And many of the entries on these lists do not have an address. And so if you have to screen an entity in China, and you don't have a street address, you are in a difficult position.

Secondly, these restricted-parties lists do not include translations into foreign languages of the names of the targeted party. The U.S. publishes its list only in English. This is of no use in China. So if you had a law-abiding company in China that wanted to screen against military end users, they have to translate on their own initiative from English to Chinese, match that against the Chinese name, and hope that they have succeeded in an accurate translation. They may not have.

So I think it would help a great deal if the government would propose with a sanction, its translation. In Dubai they would translate it into Farsi and Arabic.

Mr. BOOZMAN. Thank you, Mr. Chairman.

Mr. SHERMAN. Thank you. Mr. Tancredo?

Mr. TANCREDO. Only a couple of questions, quick questions.

When we actually do use a destination of diversion proposal, when we put that into effect, what are the ramifications of that exactly, Mr. Shulman?

Mr. SHULMAN. Well, sir, the way that the Commerce Department put together its version of this proposal, the rule would allow Commerce to impose additional restrictions on countries that are so designated. Some examples are given of the form such restrictions could take. There are no, you know, it would be decided on an individual basis for each designated country.

So in the case of the UAE, for example, we think that it would be worthwhile to treat the UAE the same way, for example, that Pakistan is treated under the Export Administration Regulations for control of items that are considered risky for diversion for nuclear proliferation purposes.

Mr. TANCREDO. But it is my understanding from testimony so far that there isn't a great deal of interest in the Department at the administration level to actually implement this. Why would they be trusted, I guess, in coming up with the criteria necessary for effective management?

Mr. SHULMAN. Sir, this is precisely why we are now recommending that this change be implemented through legislation.

Mr. TANCREDO. But, okay. So legislation then is what is, it does provide the specific way in which, in which a country that is designated as a, what is it called, destination of diversion, it specifically determines how that would be treated.

Just tell me what would happen in the UAE if, in fact, this designation were made.

Mr. SHULMAN. For example, in the UAE, the Export Administration Regulations that control the exports of dual-use goods have a special group which contains countries that are considered to be at risk for nuclear proliferation reasons.

Pakistan is listed in that group, as is Iran. The UAE is not, even though the UAE is used by both of those countries to divert goods for nuclear purposes.

So one thing that could be done is UAE could be placed in that group. And therefore, exports that are controlled for nuclear purposes to that set of countries would also be controlled to the UAE.

Mr. TANCREDO. I see. Okay, thank you very much. Thank you, Mr. Chairman.

Mr. SHERMAN. Mr. Tancredo, who has requested these hearings, co-sponsored the legislation that we are—

Mr. TANCREDO. A different Italian. A different Italian, I think. [Laughter.]

Mr. SHERMAN. Mr. Manzullo, I believe it is your turn. I do note that I believe the Asian Subcommittee is meeting right now, as well.

Mr. MANZULLO. That is correct. First of all, I want to, Mr. Chairman, I want to thank you. This is the third major bill that we have worked on, on a non-partisan basis, really enhancing the ability of America's manufacturers to help export their items expeditiously. 17-C, the DDTC bill that was moved out of committee, and now this bill.

These are, for those of us that spend our lives working on manufacturing issues, to get excited about things like this, some people

may think that, you know, these guys are, that these guys need a life. But to somebody like myself, who spends probably three quarters of his time working on manufacturing issues, because the district I represent has over 2500 industries.

And the legislation came about really as a result of a consensus with the folks involved in freight forwarding. The manufacturers themselves to whom I am the closest, because they are my constituents. The administration always wanted to make sure that the free flow of products occurs to the extent possible, obviously without compromising national security.

And Chairman, I want to thank you and the committee staff for hours and hours of work, and also the respective organizations that really sat down and tackled the problem. This will greatly enhance the ability of our exporters to get their goods overseas. But this is important; it helps out the smaller guys, who are absolutely terrified to get involved in exports, because they just don't know where to start.

With this bill and the ability to have a flag raised right at the beginning of the export process, as opposed to exporting in the dark only to have the object seized, and then a penalty and even, you know, being barred from exporting further items, this goes a long, long way.

And I don't have any questions for you, because everybody here agrees of the need that it is necessary. But you know, this is one of those times when the American people should take a little bit different view as to what happens here in Washington. Enough mischief goes on in this city.

When people from various backgrounds, different parties, different philosophies, sit down, work together on the three bills that I have mentioned, that is going a long way.

Mr. Chairman, I just want to thank you for holding this hearing. I want to thank the chairman of our full committee for being open to it. And I want to thank you, the panelists, for coming here to discuss the issue, and to give us even better ideas as to possibly what needs to be tweaked in the bill before it actually passes committee.

Thank you.

Mr. SHERMAN. I want to thank you for focusing our attention on this, which is so important, not only to our companies and jobs, but also everything we do that restricts high-technology exports, appropriate arms exports, appropriate dual-use exports. It means that those customers go to someone else. Not only does that mean we lose jobs, it also means that munitions and high-technology capacities are developed in other countries.

And we can argue about what we should restrict coming out of our country. But if you build that same industrial base in Russia, then it doesn't matter what restrictions we have; the wrong people are going to get the dangerous materials.

We have a CRS report that says that the bill might cost \$10 million, \$3 million to compile various restricted-party lists into one database, and \$7 to configure and program the system. I am going to ask—and CRS doesn't reach this on their own, but rather says that they get that from a particular source.

Two questions. Is this a realistic estimate in your opinion? And putting aside whether it is a realistic estimate, is it worth \$10 million to accomplish these goals? Let us go quickly down the witness list. Mr. Menefee.

Mr. MENEFE. Thank you, Mr. Chairman. I think it is on the high side. I think it would cost less. I think it is possible for the government, in partnership with industry, to work this out better.

Mr. SHERMAN. Okay, you think it is on the high side. If it did cost \$10 million, is it worth it?

Mr. MENEFE. Absolutely. Because if you can prevent a couple of transactions, you are well ahead.

Mr. SHERMAN. Mr. Powell.

Mr. POWELL. Absolutely worth every penny.

Mr. SHERMAN. Mr. Shulman, your organization has actually done some of the work in this area that the government should be doing, so you actually have some experiences. First, is the cost estimate, in your opinion, in the ballpark? And second, assuming it does cost \$10 million, because government always costs more than what should be in the ballpark, is it worth it?

Mr. SHULMAN. I am hoping it can be done for \$10 million, and it is most definitely worth it.

Mr. SHERMAN. Okay. Mr. Powell and Mr. Menefee are supporters of this bill. You sat here while Mr. Borman pointed to one difficulty in carrying it out; namely, that the world uses the age-old system for reporting trade, the harmonized system of tariffs to classify goods. The system doesn't really match up with our export control categories; thus, an Automated Export System would have difficulty lining up a license number with a certain HST, harmonized system of tariffs, code.

Is there a way to address this problem? And is it realistic to be able to harmonize an HST number on the one hand, and our arms control and technology control system on the other?

Mr. MENEFE. I think it is possible to do. The lists are not going to match up perfectly.

Industry has already done this. Many companies have posted on their Web site the HTS number and the export control number for their parts.

Mr. SHERMAN. So not only is it doable, it has been done. Industry may have done a better job than government can do, but until government does it there is not an official list.

Mr. MENEFE. Yes.

Mr. SHERMAN. I mean, I could go to one of these company Web sites that publishes a very useful list, just as Mr. Shulman's organization does, and if the government would just steal your list and put their official seal on it, it would be both stealing intellectual property and enhancing the purpose of your work.

Mr. Shulman, you have talked to us a little bit about the United Arab Emirates. You have talked about perhaps Congress taking action. To put them in another category, obviously any bill like that would be vetoed by this administration. Of course, we could have a bill ready to go in the future.

Other than legislation you know would be vetoed, what do you suggest we do, or within reason, push the administration to do?

Mr. SHULMAN. Mr. Chairman, I think the subcommittee should discuss that issue further with the Commerce Department; inquire why the proposal is not moving, request specific information about improvements that have been made, request that such information be made public.

Because again, as far as we are aware, there have not been substantial changes since the UAE implemented its export control law, and the proposal was halted.

Mr. SHERMAN. Sometimes I think the non-governmental panel should go before the governmental panel, and then tee up for us the really good questions to ask the governmental panel. I don't see them here. We could bring them back but we will pass on those questions.

Now, have the three of you or the organizations that you represent, met to discuss this bill? I realize that Mr. Shulman's organization comes at it from a different angle. He has got some suggestions for the bill; he has put them forward here. I hope you gentlemen have seen them before.

What do you think of his ideas?

Mr. MENEFFEE. I think, by and large, they are good ideas.

Mr. POWELL. I would agree.

Mr. SHERMAN. Okay. So we could reach a consensus between the export control/national security world and the business world, and we would still face some opposition from the administration, mostly concerned about cost. But you know, given what it costs to fight a war, what it costs when just one improvised explosive device with the explosively formed projectiles goes off, this is so cheap compared to dealing with the effects of making the wrong decision that I, for one, would like to see us spend \$10 million more to improve both the efficiency of the system and its capacity.

I think then I am out of questions. And, Mr. Royce.

Mr. ROYCE. Thank you, Mr. Chairman. I am going to ask Mr. Shulman a question which I think goes to the, kind of the bottom line of the problem here.

As many times as I think I have turned this thing off, Mr. Chairman.

Mr. SHERMAN. Clearly it would cost more than \$10 million to get this technology fixed if individual Members of Congress were involved.

Mr. ROYCE. Yes. I am glad I am not on that end of the engineering.

But Mr. Shulman, you express great concerns that the validated end-user program in China has been abused, citing links between approved companies and the Chinese military. So I was going to ask you, do you think it is possible in general to keep dual-use technology exports in China secure?

Mr. SHULMAN. I certainly believe that it is possible to keep them more secure, and not enough is being done by the administration to do that.

Mr. ROYCE. Let us talk about how, and how in this bill you would solve that problem. I mean, if the basic problem is that the military itself is a business partner, as you cite in your testimony, in these business deals, then how do we ensure our objective here?

Mr. SHULMAN. The links to the Chinese military were a bit more attenuated in the two cases that we cited and that we found.

However, it is our impression that this program, particularly the first five entities that were designated under it, should have been the purest of the pure that could be found in China. And this apparently was not the case.

Mr. ROYCE. Well, I guess that begs the question, if you are looking at the purest of the pure, and you are still finding those BLA ties, or military ties, then is the situation so endemic, is the situation so pervasive that virtually any type of program is going to end up being corrupted by the intentions of the military industrial complex in China? That they will be able to get access to this dual-use technology.

Mr. SHULMAN. Sir, it is certainly a risk. And this is why our strong preference is for the standard licensing process to be used in the case of China, to ensure that individual exports are viewed individually, for those reasons.

Mr. ROYCE. Then how do we do more on the end-use checks to make sure that that happens? If you were pounding out this legislation, how would you lay out the end-use checks to make certain we reach that objective?

Mr. SHULMAN. Well, certainly we think that more resources could be devoted to carrying out end-use visits, to continue to negotiate with the Chinese Government, to have more effective inspections. Little-notice or no-notice inspections, et cetera. There are many things that could be done, and that is also a very good investment.

Mr. ROYCE. Explain how we would do that if the Chinese authorities stiff our investigators. Isn't that part of the problem?

Mr. SHULMAN. In that case, it may be better not to allow the export, sir.

Mr. ROYCE. Not to allow the export, right?

Mr. SHULMAN. Yes, sir.

Mr. ROYCE. Right. All right. Well, let me go to one other question, Mr. Chairman, that I was going to ask. And that was something that Mr. Powell said in his testimony.

You said that H.R. 5228 is clearly cognizant of the differences between small, medium, and large exporters. I was going to ask how so? Do you mean it favors one class of exporter over the other? What did you mean by that?

Mr. POWELL. Well, I think the larger exporter has more assets available from within, just by virtue of their size and configuration. And it was mentioned connectivity between the harmonized number and the ECCN number is out in business today, but in your large typical companies.

We are all aware that 50 percent of the GDP of the United States is created by small businesses; and in fact, the growth is coming from small business today. And small business is afraid to get into exports, by virtue of being I would say confronted with penalties due to lack of knowledge and so forth.

And H.R. 5828 would go just a tremendous way to increase exporters from the United States, qualified exporters from the United States, which obviously helps trade deficits and all these other little things.

So it goes deep to get the smaller people involved. And H.R. 5828 does that, if that answers your question, sir.

Mr. ROYCE. That does. I appreciate that.

Well, Mr. Chairman, I think that is all the questions I have.

Mr. SHERMAN. I am going to request that perhaps the three of you, or at least the organizations that you represent, together with staff of the subcommittee and perhaps Mr. Manzullo's staff, whether it would be Mr. Royce's staff or Mr. Manzullo's staff or both, sit down and try to work out improvements to this bill.

Sitting behind me is the staff director of the subcommittee, Mr. Don McDonald. And he will put it together. Because I think this bill goes in the right direction. There may be one or two issues that need to be resolved in a markup. We should get input from the Department of Commerce on the one issue that they had; try to get some of Mr. Shulman's ideas in; and see if we can't come to something close to a consensus bill before we mark this bill up.

But I think that there is enough time between now and the summer break to get this bill passed through the subcommittee, the committee, and the floor. And then the next issue is the United States Senate. There has got to be a reason why Coleman would, why the Senator from Oklahoma would put a hold on this, because he has put a hold on all out other bills. But we will overcome them.

And with that, we stand adjourned.

[Whereupon, at 11:37 a.m., the subcommittee was adjourned.]

