TESTIMONY OF ARTHUR SHULMAN
GENERAL COUNSEL
WISCONSIN PROJECT ON NUCLEAR ARMS CONTROL

Hearing on the Export Administration Act:
A Review of Outstanding Policy Considerations

House Committee on Foreign Affairs
Subcommittee on Terrorism, Nonproliferation, and Trade

June 18, 2009

I am pleased to appear before this distinguished Subcommittee to discuss dual-use export controls, and their role in stemming the spread of mass destruction weapons.

I will cover four topics. First, the importance of strong and effective export controls for U.S. national security; second, the resources and authorities required to enable our export control officials to do their jobs properly; third, the need to improve industry's ability to police itself; and fourth, ways to address the risks of transshipment and diversion at home and abroad.

A matter of national security

The Export Administration Act (EAA) is the foundation of our system for controlling the export of dual-use, militarily sensitive technologies from the United States. For most of the last two decades, this key statute has been in lapse. The dual-use export control system has continued to operate on an emergency basis, under the authority of the International Emergency Economic Powers Act (IEEPA). Efforts to reauthorize the EAA have been driven by industry, seeking to lower controls under the guise of "modernizing" the system and making it less "burdensome" and more "efficient." The Export Administration Act remains in lapse because Congress, in its wisdom, has refused to undermine our national security by adopting these proposals.

Are dual-use export controls a burden on U.S. industry? The facts speak for themselves. An analysis by the Government Accountability Office (GAO) showed that in 2005, 99.81 percent of exports subject to the Export Administration Regulations (EAR) left the United States without an export license, including 98.5 percent of items on the Commerce Control List. And even for the tiny fraction of dual-use trade that required an export license, the Commerce Department denied only 1.4 percent of the license applications it processed during that period (FY2005), while lowering processing times. Two years later, denials were at 0.88 percent. One almost wonders, what's left for industry to complain about?

The focus of export control reforms should be on ensuring that the system protects U.S. national security in the 21st century – not on removing the remaining speed bumps on the export superhighway. While the EAA has been in lapse, the export control system has not been updated to reflect the post-Cold War and post-9/11 security environment. The GAO has lamented the absence of a comprehensive, public analysis of the current security challenges, how the dual-use export control system is meeting these challenges, and what changes are needed. Commerce apparently

conducted an ad hoc review after the events of September 2001, but decided that no fundamental changes were needed. Thanks to the efforts of this Subcommittee, our nation's arms exports will be subjected to a comprehensive national security review if H.R. 2410 becomes law. The same must be done for dual-use trade. Only then would we have the hard data needed for thinking about a new Export Administration Act – one that would protect our security in the present and future.

In the interim, we must ensure that the current system is working well to protect us. In many ways, it is not, but there are things we can do now to change that. Congress should give the Bureau of Industry and Security (BIS) at Commerce enough resources to do the job it has now. Congress should also provide robust oversight to ensure that those resources are being used well.

More for Export Enforcement

I would like to note a recent article by Darryl Jackson, formerly Assistant Secretary of Commerce for Export Enforcement. Mr. Jackson notes the need for the dual-use export enforcement officials in the Bureau of Industry and Security to carry out their crucial mission with "maximum effectiveness." Export enforcement agents need to be able to conduct investigations abroad, to go undercover and to set up wiretaps, to deter and punish criminals by seizing profits and assessing higher penalties. Mr. Jackson suggests that Congress pass a standalone bill immediately that would give OEE permanent law enforcement authority. This Subcommittee introduced just such a provision last year in H.R. 6828, and should do so again in this new Congress.

Another issue is that BIS export enforcers do not have sufficient personnel and funding. At present, OEE has more than 800 open cases - but fewer than 100 special agents to work them, throughout the country. These staffing and resource levels have remained static for years – but violators have not. The budget request for FY2010 would provide an additional 3 persons to OEE. That is a start, but not enough. Additional staff and resources for enforcement should be a priority for Congress.

Safer Export Administration

Additional resources would also help with another problem. During several lean years, BIS has tried to shrink its workload by doing away with license requirements. An example is the "Validated End-User" (VEU) program, which I discussed in my testimony before this Subcommittee last year. Launched in 2007, the program allows select foreign companies to receive controlled dual-use goods without otherwise-required export licenses. An interagency committee is supposed to choose companies and locations posing little or no risk of diversion. But our initial report on the program, published in January 2008, revealed that two of the first five Chinese companies designated as VEUs were 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. BIS hand-picked those companies, tellingly noting that they accounted for 18% of licensed U.S. exports to China. And BIS reportedly estimated that the next batch of five Chinese VEU candidates would account for 90 percent of exports to China subject to BIS licensing, when combined with the original five VEUs. Since then, one additional VEU was designated in April (the other four candidates are presumably still in the pipeline). My organization analyzed this designation, and our analysis revealed that components useful in gas centrifuge enrichment plants

can now be shipped, without limits or prior scrutiny, to a building that houses the headquarters of a Chinese company which, as recently as December, was under U.S. sanctions for proliferation to Iran and/or Syria. I ask that this analysis be made part of the record for this hearing.

The VEU program has been not only a selection failure but also a verification cripple. In January, BIS finally secured Chinese consent to the post-shipment inspections required under the program. That's eighteen months after the program's launch, and over a year after the first VEUs were freed to receive sensitive exports license-free. In the interim, the GAO highlighted the risk of unverified license-free exports and pointed out other flaws in the program. Yet even now, on-site VEU reviews require a 60-day notice and must be arranged and accompanied by Chinese government officials.

Given these fundamental flaws and limitations, the VEU scheme should be scrapped. At the very least, a moratorium on new designations should be imposed, as Congress studies whether the program can operate without undermining our security. The VEU program and other "trusted customer" initiatives 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 even more 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. Congress should scrutinize such initiatives closely, and ensure that they are not driven by resource shortages at BIS.

More help for industry to protect our national security

Industry is the first line of defense in our current system for controlling militarily useful trade. Nevertheless, industry is still not getting enough help from the government in safeguarding our safety. One 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 – especially to mass destruction weapon programs around the world. An exporter usually must apply to BIS for a license before selling a controlled item to an entity on the List. But, as I explained in my testimony last year, the List is incomplete and out of date, especially its China section. Some entries are now inaccurate, and others are not usable.

Despite criticism from auditors and requests from industry and national security advocates, little has been done to improve the List. My organization has submitted to BIS concrete proposals for updating this crucial national security resource. Last year, we grew tired of waiting and 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 addresses.

Despite our hopes, however, BIS has made none of these changes. The agency did finally commit to annual reviews of the List. But so far, the review process has only resulted in removals of listed entities. The agency has also instituted a formal petition process for removal from the list – and has already removed one company as a result. There is no corresponding public procedure to request addition of risky end-users. BIS has also begun to use the List to identify entities not directly linked to proliferation or to terrorism, but implicated in various smuggling networks, for example. So, the List now has more names, but it is not more accurate or clear, and has lost its focus

on nonproliferation. Congress should press BIS to make the Entity List a real tool for exporters to screen their transactions and prevent diversions.

Combating Illicit Transshipment and Diversion

This Subcommittee has taken a leadership role in addressing the risks of transshipment and diversion of dual-use U.S. goods. Last year, I testified about the history of illicit transshipment through the United Arab Emirates (UAE). I would like to offer for inclusion in the hearing record an updated chronology documenting how Dubai and other points in the UAE have served for decades as the main hubs in the world for nuclear and other smuggling. Authorities in the United States and elsewhere are still bringing criminal cases against smugglers shipping dangerous goods through the UAE. We have also seen such activity channeled through Malaysia and other countries with weak export controls – expanding the geography of this threat.

A recent GAO investigation highlighted another aspect of the problem – domestic sales. Using a credit card and little else, the GAO was able to buy a variety of highly sensitive items controlled for export, including switches usable for triggering nuclear weapons. Since the items were first delivered within the United States, little or no scrutiny of the sales was required by law. Then, the investigators shipped dummy versions of the items to a country known as a transshipment and diversion point, entirely evading customs scrutiny of the exports. This operation reproduced a scheme used repeatedly by those intent on illicit acquisition of controlled dual-use technology from the United States.

There are things we can do to meet these challenges. For instance, additional resources would allow BIS to expand its successful program of outreach visits to industry – particularly smaller businesses. Such visits increase awareness of export control requirements and diversion threats, and often lead to tips about suspicious acquisition attempts. In addition, BIS must get more staff and resources to verify abroad that exported sensitive technology ends up and remains in authorized locations and uses. And both Customs agencies should be given direction and resources to prioritize export control review of outgoing shipments and verification of industry self-policing activities.

Revisions to the Automated Export System (AES) proposed by this Subcommittee last year in H.R. 6828 also hold great potential. Mandatory, real-time linkages and automated cross referencing could be set up between export license data, shipment information and enforcement records. Such automation would make work by export compliance and enforcement officials much more efficient, by flagging problem transactions for investigation before they cross the border. The AES revisions would also help exporters, by facilitating classification decisions and by automatically screening transactions against restricted party lists. Such services are now available commercially, but they are too expensive for smaller businesses. Government should make these crucial decisions easier for exporters, without relieving them of responsibility for knowing their products and customers.

We should also do all we can to encourage systematic reporting by industry of suspicious acquisition attempts. So far, only a handful of individual companies in Europe and the United States have established such relationships with their regulators. Systematic reporting by industry would generate a tremendous amount of data, which could be analyzed and used to uncover and defeat

proliferation networks. Industry should also be incentivized to embed anti-diversion technology – including tracking chips and immobilizers – in sensitive equipment controlled for export. A few companies do this already, but more widespread adoption of such measures must be encouraged. On the other hand, robust enforcement and heavy penalties must also be maintained, to punish criminals and to deter the reckless and the would-be violators.

Finally, the United States should do more to convince our friends and allies to maintain effective controls on strategic trade, and to supply practical training and assistance to countries trying to do a better job. But those who refuse to do their part, and who facilitate dangerous trade through their territories, should not be spared. The UAE continues to be a problem in this regard. The Mayrow network was based there, allegedly sending to Iran U.S.-origin components used to make the improvised explosive devices killing our soldiers in Iraq and Afghanistan. Iran continues to import large quantities of goods through Dubai's revolving door, posing a grave security risk and circumventing sanctions efforts. Congress must continue to demand real export control improvements by the UAE, and should attach conditions to that effect to any agreement for nuclear cooperation. At the same time, we need broader tools to motivate and punish countries which do not adopt effective export controls as required by United Nations Security Council resolution 1540. Congress should legislate the “destinations of diversion concern” concept, which would impose greater controls on trade with such diversion facilitators.

Oversight remains necessary

The challenges I’ve discussed – the flawed VEU program, weak Entity List, and others – have been exposed and publicized through the work of this Subcommittee and others. Congress should expand and systematize this oversight, and enlist other investigators to help it. For example, the GAO should be tasked with reviewing export records and BIS licensing decisions every year. Such reviews generate valuable data for checking whether the system is protecting our security.

Congress should also use help from the relevant Inspectors General. Until recently, 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.