

EXPORT-CONTROL REFORM

BUSINESS EXECUTIVES FOR NATIONAL SECURITY

WASHINGTON, DC

APRIL 20, 2010 – 1:30 PM

My thanks to Business Executives for National Security for hosting this event. In areas like accounting, procurement, privatization, and excess base structure, BENS has identified problems and proposed solutions that have saved the taxpayers billions of dollars and made our military a more effective fighting force. As many of you know, for the better part of three years now I have spoken out at various times about the need to adapt and reform America's national-security apparatus to better deal with the realities of the post-Cold War era.

Some of those necessary shifts include:

- Enhancing America's civilian instruments of national power – above all diplomacy and development – and better integrating them with our military;
- Rebalancing the defense establishment to reflect the lessons learned and capabilities gained from recent conflicts, especially counterinsurgency, stability, and reconstruction operations;
- And, most recently, reforming the way we build the capacity of allies and partners to better fight alongside us and secure their own territory.

All these institutional shifts are, to one degree or another, aimed at improving the way the United States works with and through other countries to confront shared security challenges.

So is the matter I would like to discuss today: the need to reform the U.S. government's regulations and procedures for exporting weapons and so called dual-use equipment and technology. Earlier this year, the president announced that he would seek to further enhance our national security through substantial changes to our export-control regime. He did so with the unanimous support of his entire national-security team. This afternoon I will focus on what I believe are the compelling security arguments for the changes recommended by the president.

I want to state from the outset how critically important it is to have a vigorous, comprehensive export-control system that prevents adversaries from getting access to technology or equipment that could be used against us.

The problem we face is that the current system – which has not been significantly altered since the end of the Cold War – originated and evolved in a very different era, with a

very different array of concerns in mind. As a result, its rules, organizations, and processes are not set up to deal effectively with those situations that could do us the most harm in the 21st Century – a terrorist group obtaining a critical component for a weapon of mass destruction, or a rogue state seeking advanced ballistic-missile parts. Most importantly, the current arrangement fails at the critical task of preventing harmful exports while facilitating useful ones.

The United States is thought to have one of the most stringent export regimes in the world. But stringent is not the same as effective. A number of lapses in recent years – from highly sensitive materials being exported to vital homeland security capabilities being delayed – have underscored the flaws of the current approach.

Several factors contribute to these kinds of scenarios, which at worst could lead to the wrong technology falling into the wrong hands. One major culprit is an overly broad definition of what should be subject to export classification and control. The real-world effect is to make it more difficult to focus on those items and technologies that truly need to stay in this country. Frederick the Great's famous maxim that "he who defends everything defends nothing" certainly applies to export control.

This problem goes back a long way, and was evident even before the collapse of the Soviet Union. In 1982, when I became deputy director for intelligence at CIA, my responsibilities included tracking prohibited transfers of U.S. technology. It soon became apparent that the length of the list of controlled technologies outstripped our finite intelligence monitoring capabilities and resources. It had the effect of undercutting our efforts to control the critical items. We were wasting our time and resources tracking technologies you could buy at RadioShack.

Today, the U.S. government reviews tens of thousands of license applications for export to EU and NATO countries. In well over 95 percent of these cases, we say "yes" to the export. Additionally, many parts and components of a major piece of defense equipment – such as a combat vehicle or aircraft – require their own export licenses. It makes little sense to use the same lengthy process to control the export of every latch, wire, and lug nut for a piece of equipment like the F-16, when we have already approved the export of the whole aircraft.

In short, the time for change is long overdue if the application of controls on key items and technologies is to have any meaning. We need a system that dispenses with the 95 percent of "easy" cases and lets us concentrate our resources on the remaining 5 percent. By doing so, we will be better able to monitor and enforce controls on technology transfers with real security implications while helping to speed the provision of equipment to allies and partners who fight alongside us in coalition operations. A second major obstacle we face is the bureaucratic apparatus that has grown up around export control – a byzantine amalgam of authorities, roles, and missions scattered around different parts of the federal government. In theory, this provides checks and balances – the idea being that security concerns, customarily represented by DoD, would check economic interests represented by the Commerce Department and balance out diplomatic

and relationship-building equities represented by State. In reality, this diffusion of authority – where separate export-control lists are maintained by different agencies – results in confusion about jurisdiction and approval, on the part of companies and government officials alike.

It creates more opportunities for mistakes, enforcement lapses, and circumvention strategies such as "forum shopping," where exporters with problematic license applications try different agencies looking for the best result. In one instance, an individual was caught intentionally exporting a controlled item without a license, but escaped prosecution by presenting two conflicting determinations from two different government agencies. The item in question was a carbon composite material used in ICBM nose cones.

As a result of this dispersed arrangement, the U.S. government spends an enormous amount of time and energy on what are essentially process questions – trying to decide which agency has jurisdiction – as opposed to the more important issue of whether a given technology can be safely exported. These internal squabbles can have real world consequences. A fight between agencies over jurisdiction, for example, delayed a program to place new screening equipment in U.S. and overseas airports.

Correspondingly, many companies face a frustrating situation where an exporter with a single purchase order may have to seek licenses from two separate agencies, and could be approved by one but denied by the other. Additionally, because it is so difficult to modify or update the control lists, a controlled item might never be considered for a lower level of restriction even if it becomes much less sensitive and important over time. The system has the effect of discouraging exporters from approaching the process as intended. Multinational companies can move production offshore, eroding our defense industrial base, undermining our control regimes in the process, not to mention losing American jobs. Some European satellite manufacturers even market their products as being not subject to U.S. export controls, thus drawing overseas not only potential customers, but some of the best scientists and engineers as well. At the same time, onerous and complicated restrictions too often fail to prevent weapons and technologies from going places they shouldn't. They only incentivize more creative circumvention strategies – on the part of foreign companies, as well as countries that do not have our best interests at heart.

Concurrently, we have not updated our system to deal with the U.S. military's transition to off-the-shelf procurement. More and more, our military is taking advantage of commercially manufactured items, presenting challenges when determining whether or not a given technology is acceptable for export. There are electronic components used in many third-generation cellular devices that are also important components of sophisticated stealth-defeating radar systems. We need to update our export-control system to reflect these new realities. Finally, the current export-control regime impedes the effectiveness of our closest military allies, tests their patience and goodwill, and hinders their ability to coordinate with U.S. forces – this at a time when we count on allies and partners to fight with us in places like Afghanistan and potentially elsewhere.

Not too long ago, a British C-17 spent hours disabled on the ground in Australia – not because the needed part wasn't available, but because U.S. law required the Australians to seek U.S. permission before doing the repair. These are two of our very strongest allies for God's sake! Similarly, close, long-standing allies and partners like South Korea have bought U.S. aircraft only to encounter difficulties and delays in getting spare parts – something that weakens our bilateral relationships, our credibility, and ultimately American security.

That is one of the reasons why several U.S. secretaries of defense representing multiple administrations of both political parties have voiced frustration over the export-control system. As defense secretaries, we have all, at one time or another, had to sit across the table from defense ministers from important allies or new partners and explain why the U.S. government is unable to follow through expeditiously on its commitments to provide the weapons, equipment, and support they have been promised and have paid for. It is not an edifying experience. All the while, other countries that do not suffer from our encumbrances are taking the opportunity to sell weapons, build relationships, and improve their strategic position and economic standing. Some obstacles to having a strategically sound defense trade relationship can be addressed through bilateral agreements with our closest allies and partners. In 2007, the U.S. signed Defense Trade Cooperation Treaties with both the United Kingdom and Australia – treaties that still await ratification in the U.S. Senate. Through streamlined export-control arrangements and enhanced technology security measures, these agreements would substantially improve our ability to equip and support U.S., U.K., and Australian forces deploying in combat operations. They contain provisions allowing for the establishment of export-authorized groups of U.S., U.K., and Australian companies. Except for a short list of truly critical equipment and technologies, these trusted companies could largely avoid individual export licenses. I remain hopeful that the Senate will give advice and consent to both of these treaties prior to the summer recess.

The kinds of common sense changes contained in the U.K. and Australia treaties are a step in the right direction, at least with these two key allies. But international agreements are still no substitute for the kind of fundamental systematic reform of export control that this country urgently needs. The fact is, for all the reasons I described earlier, America's decades-old, bureaucratically labyrinthine system does not serve our 21st-century security needs or our economic interests. It is clear our current limitations in this area undermine America's ability to work with and through partners to confront shared threats and challenges – from terrorism to rogue states to rising powers. Our security interests would be far better served by a more agile, transparent, predictable, and efficient regime. Tinkering around the edges of our current system will not do. For these reasons and more, in August of last year, the president directed a broad-based review of the U.S. export-control regime. He has called for reforms that focus controls on key technologies and items that pose the greatest national-security threat. These include items and technologies related to global terrorism, the proliferation and delivery systems of weapons of mass destruction, and advanced conventional weapons. In short, a system where higher walls are placed around fewer, more critical items.

Following this directive, and informed by a recent National Intelligence Council assessment of the key national-security considerations, I have worked closely with my counterparts at the departments of State, Commerce, Homeland Security, as well as with the director of national intelligence and the national security advisor to develop a blueprint for such a system. Our plan relies on four key reforms: a single export-control list, a single licensing agency, a single enforcement-coordination agency, and a single information-technology system. First, a single export-control list will make it clear to U.S. companies which items require licenses for export and which do not. This single list, combined with a single licensing agency, would allow us to concentrate on controlling those critical technologies and items – the "Crown Jewels" – that are the basis for maintaining our military technology advantage, especially technologies and items that no foreign government or company can duplicate. Items that have no significant military impact, or that use widely available technology, could be approved for export quickly. We envision a more dynamic, tiered control system where an item or technology would be "cascaded" from a higher to a lower level of control as its sensitivity decreases.

Second, a single licensing agency, which will have jurisdiction over both munitions and dual-use items and technologies, will streamline the review process and ensure that export decisions are consistent and made based on the real capabilities of the technology. This agency would also reduce exporters' current confusion over where and how to submit export-license applications, as well as which technologies and items are likely to be approved. The administration is currently preparing options for the agency's location, and I anticipate a presidential decision later this spring.

Third, the coordination of our currently dispersed enforcement resources by one agency will do a great deal to strengthen enforcement, particularly abroad, as well as coordination with the intelligence community. Those who endanger our troops and compromise our national security will not be able to hide behind jurisdictional uncertainties or game the system. Violators will be subject to thorough investigation, prosecution, and punishment severe enough to deter lawbreaking.

Fourth, a single, unified IT infrastructure will reduce the redundancies, incompatibilities, and waste of taxpayer money that our current system of multiple databases produces. For example, a single online location and database would receive, process, and help screen new license applications and end-users. Of course, the question of which end-users are eligible to receive our technology is a critical national-security concern. An essential component of the reformed system is the list of entities – terrorist organizations, rogue states, and others – that cannot be allowed access to sensitive items. This would deny them technology or force them to acquire it through more difficult routes. In order to facilitate compliance and tracking, we propose to consolidate current lists of banned end-users into one single frequently-updated list that will be easy for those performing transfers to consult. Entities can be added at any time if there is reasonable cause to believe they are involved in activities contrary to U.S. national-security interests. These fundamental reforms, if enacted together, will improve America's ability to work with and fight alongside allies and partners by setting clear, transparent standards – standards that will make it possible to share technology more freely, especially items needed and

used by all of us to counter common threats. I'd like to emphasize that the new system will be in full compliance with all of our existing multilateral treaties and obligations. The prospect of more defense trade with the U.S. will incentivize other nations to strengthen their own export regimes. Given how quickly and easily goods and information now can move around the world, export controls are far more effective when they involve multiple partners with shared interests and values.

As happens with any major reform to an entrenched, long-standing system, there will be resistance and criticism. Some people will be concerned that having fewer items subject to the most onerous export restrictions will make it easier for hostile states or groups to obtain weaponry and technology that potentially could be used against us. No system – above all, the current one – is foolproof. But by consolidating most export licensing functions in one agency and creating an enforcement coordination agency, we can focus our energies and scrutiny on technologies that truly threaten American security, making it far less likely that these critical items will fall into the wrong hands. It is also important to bear in mind that the U.S. government will retain the ability to impose economic sanctions on any foreign country or group, to include prohibiting the export of any equipment, material, or technologies that could have military use. We will turn these principles and proposals into action through a three-phased process that will unfold over the course of the next year. In the first phase, the executive branch begins the transition towards the single list and single licensing agency by making significant improvements to the current system. These efforts would include establishing criteria for a tiered control list and standing up an integrated enforcement center. The second phase completes the transition to a single IT structure, implements the tiered control list, and makes substantial progress towards a single licensing system.

These changes, which can be made through executive action, represent substantial progress and momentum towards reform. But they are by themselves insufficient to fully meet the challenge at hand. We need a final, third phase – a thorough overhaul of the current system along the lines I have described today, most notably the single licensing agency and single enforcement coordination agency. These fundamental changes will require congressional action.

I greatly appreciated the chance to meet with a number of senior members of Congress earlier this year to discuss this topic. I valued the feedback and suggestions they provided at the time, and I look forward to further dialogue. It is the president's hope that his national-security team can continue to work closely with congressional leaders and all of the key committees to turn these proposals into legislation that the president can sign sometime this year.

I know that earlier attempts at reform have foundered in the face of resistance. The proposition that a more focused and streamlined system actually helps our national security can go against conventional wisdom. But for the reasons I've described today, I believe it is the right approach, and it is urgently needed given the harmful effects of continuing with the existing set of outdated processes, institutions, and assumptions.

Indeed, America's ability to engage effectively with the rest of the world and keep our most sensitive technology away from those who would do us harm depend critically on our ability to get this right. I look forward to working with the Congress and my interagency colleagues to achieve the kind of systematic reform that will benefit both the security and prosperity of the American people. Thank you.

###