Testimony of

Andrew Howell, Vice President for Homeland Security Policy
United States Chamber of Commerce

"The Future of Port Security: The GreenLane Maritime Cargo Security Act"

Before the

Senate Committee on Homeland Security & Government Affairs

April 5, 2006

Introduction

I would like to thank Senator Collins, Senator Lieberman, and all the Members of this Committee for giving me the opportunity to testify before you today.

My name is Andrew Howell, Vice President for Homeland Security Policy at the United States Chamber of Commerce. The U.S. Chamber of Commerce ("the Chamber") is the world's largest business federation, representing more than 3 million businesses through our federation, which includes direct corporate members of all types and sizes; trade and professional associations; state and local chambers throughout the United States; and 104 American Chambers of Commerce abroad (AmChams) in 91 countries.

On behalf of the Chamber, I would like to express our appreciation to the Committee for having this opportunity to comment on the GreenLane Maritime Cargo Security Act. We applaud the Committee's continued efforts to bring attention to the important issue of supply chain security so that we can better defend our nation from future terrorist attacks while maintaining the vitality of the American economy. The Chamber believes that ensuring the security of our citizens should be America's first priority. We look forward to continuing to work with members of this Committee as you address this important matter.

GreenLane Cargo Security Act

We commend Chairwoman Collins and Senator Murray for taking a leadership role in addressing the very important issue of ensuring the security of the international maritime supply chain. The GreenLane Maritime Cargo Security Act by and large represents a

reasoned approach to maritime and cargo security. At the same time, we are hopeful that, working with Members of this Committee and staff, we can address some significant issues we have with this bill. However, we are most enthusiastic about your attempt through this legislation to provide incentives for businesses to adopt security practices with tangible benefits such as the expedited release of cargo and drastically reduced inspections.

This approach is consistent with the multi-layered, risk-based policy of the U.S. Department of Homeland Security ("DHS") in addressing supply chain and maritime security. The legislation builds upon the strength of successful programs already established by U.S. Customs and Border Protection ("CBP"), including the Customs Trade Partnership Against Terrorism ("C-TPAT").

CBP should be commended for engaging the trade community and foreign governments to develop and implement these programs that improve supply chain security without disrupting the flow of trade and damaging the U.S. economy.

Since shortly after 9/11 the trade community and the Federal Government have worked closely together to strengthen border security and improve the flow of low-risk cargo across U.S. borders. U.S. companies engaged in international trade have spent a great deal of time, effort, and money on improving the security of their supply chains. Congress should recognize that companies have taken, and continue to take, voluntary measures to address key security concerns at their own expense.

The Government has also actively engaged foreign nations in discussions that have allowed for the implementation programs such as the Container Security Initiative ("CSI"), which places U.S. Customs officials at foreign seaports. Moreover, the U.S. has played a key role in negotiating the World Customs Organization's Security Framework. The common element in all of these programs is that they are based on partnerships and input by all affected parties to gain successful outcomes.

Although the programs mentioned above do have room for improvement, many believe that they have individually helped improve supply chain security. When taken in aggregate, they form effective layers of improved supply chain security.

At the same time, Congress should be careful and avoid being overly prescriptive in its approach to this issue. There is no "one-size fits all" solution for improving supply chain security. Because of differences between and among industries and modes of transportation, what works for one sector or company will not work for others. The supply chain is global in nature, and we must therefore work together to find solutions that will work internationally. It is also essential that security programs remain flexible to adapt to meet not only evolving threats, but also evolving industry practices in global goods movement.

Areas of Concern

While we support the basic goals of the GreenLane Cargo Security Act, there are several key provisions of the legislation that we believe merit additional discussion and modification. In general, the legislation places too great an emphasis on C-TPAT along with GreenLane as panaceas for addressing supply chain security. It is important to remember that C-TPAT and individual programs are not the sole solution to supply chain security. These programs are part of a collection of DHS programs that, taken together, comprise a multi-layered strategy to improve supply chain security.

In particular, we disagree strongly with provisions in sections 9 and 10 of the legislation that would require the Secretary of Homeland Security to promulgate regulations that describe the minimum requirements, program tiers, and program benefits of C-TPAT and "GreenLane" respectively. We are greatly concerned that regulation will damage the cooperative nature of these programs and would actually limit their ability to evolve in an ever-changing security, economic, and technology environment.

The practical effect of requiring such rulemakings would be to convert a flexible, voluntary initiative into a regulated program. C-TPAT has worked well, and indeed continues to work well, as a voluntary partnership between government and the business community. Since its inception, the program has served as an exemplary model of how the business community can work cooperatively with government to improve security while facilitating trade. We strongly oppose any attempt to regulate C-TPAT.

Second, the legislation would authorize the government to collect information about business operations and security procedures. The legislation, in its current form, does not contain sufficient safeguards against the unwarranted distribution of information and/or data.

Third, any new security mandates placed upon the trade community will pose a unique burden upon small and medium-sized businesses, which are the job-creating machines of our economy. In particular, the legislation as written does not adequately address the regulatory compliance costs that would be imposed upon these businesses.

Finally, we question the wisdom of using private third-party entities to validate supply chain security practices of C-TPAT participants. The use of third party validators raises issues of cost, confidentiality, and practicality. Instead, we believe Congress should give CBP the necessary resources to conduct the needed validations.

Customs Trade Partnership Against Terrorism (C-TPAT)

C-TPAT continues to be effective precisely because it is a voluntary partnership, and not a regulated program. By working in a voluntary and collaborative environment, the Government and the trade community bring together experts who can openly discuss actions that add real value to supply chain security, without negatively impacting the economy.

As we have seen, government and industry develop effective guidelines that recognize the global and unique nature of supply chains (*e.g.* lanes of supply from China are inherently different from those from Africa or South America) and the differences in commodities and industries (suppliers of automotive parts vs. textile products). The nature of the program allows CBP and industry to work together to respond more quickly to future security, economic, and technological changes.

In contrast, regulation may have the unintended consequence of stifling creativity and discouraging participation in the program. For example, government, the trade community, and technology vendors have been working together to develop technological solutions that would increase cargo security. All parties have put their needs, capabilities, and possible solutions on the table. Regulations that mandate certain technological solutions could stifle such collaborative efforts to create new and better technological solutions and put C-TPAT participants at a cost disadvantage relative to non-participants.

Additionally, the government and the trade community are working together to determine what trade data will actually improve risk assessments and targeting of shipments for examination. All parties are at the table and are robustly discussing potential solutions. Regulations that mandate the content of that data may impede ongoing efforts to determine what additional data elements are needed to enhance our targeting capabilities.

On another note, C-TPAT works precisely because the U.S. government cannot effectively regulate the security practices of private companies in foreign countries. However, participating C-TPAT firms do have the ability to work with these overseas suppliers to implement secure business practices, by conditioning their business relationships upon the implementation and verification of supply chain security procedures.

Furthermore, some proponents of regulating C-TPAT wrongly contend that there are currently no baseline requirements for C-TPAT participants. On March 13, 2006, the U.S. Customs and Border Protection published minimum security criteria for C-TPAT highway carriers. Similar criteria for importers were published in March of 2005. In neither instance were these criteria the subject of federal rulemaking. C-TPAT remains a voluntary public-private partnership, albeit with specific program requirements that must be adhered to by

companies in order to receive tangible benefits. Rulemaking is simply not necessary to establish baseline criteria, and in fact, allows for effective, flexible and customized security plans based on an individual member company's business model.

GreenLane Designation

The legislation proposes to authorize the creation of a third tier of C-TPAT known as "GreenLane" that would confer additional benefits to validated C-TPAT participants that have demonstrated the highest levels of security practices. As noted earlier, the Chamber strongly supports the concept of greenlanes. Providing tiered benefits to companies that have voluntarily undertaken measures to improve their supply chain security is a fundamentally sound idea. In fact, CBP has already adopted a tiered benefits approach to C-TPAT.

However, we question the wisdom of prescribing the requirements and benefits for the GreenLane program in legislation, or even in regulation. Both the business participation and the operational success of the C-TPAT program have been premised upon the notion of flexibility. GreenLane should not deviate from this approach. To the extent that Congress seeks to establish baseline criteria for participation in GreenLane, this would best be accomplished by working cooperatively with the private sector. For example, late in 2005, the Commercial Advisory Operations Committee ("COAC") issued a report recommending tangible benefits that Customs should provide to GreenLane participants.

We would candidly prefer that CBP, using existing authority, aggressively move to make decisions on its vision of a greenlane. However, to the extent that the proposed legislation is an expression of frustration with DHS not making this decision, we agree. Firms have invested millions in enhanced security practices anticipating a future benefit from a greenlane program that has yet to materialize.

Container Security Devices

In describing the GreenLane concept last year, former Customs and Border Protection Commissioner Robert Bonner laid out the basic requirements that C-TPAT participants must undergo in order to achieve true green lane status, that is "no inspection upon arrival—immediate release." Most critical among these requirements is the use of smart box technology that can detect and record whether tampering has occurred with a container seal after being affixed at the point of origin.

This smart box technology, referenced in section 10 of legislation as "Container Security Devices" ("CSD") is a critical element to making the GreenLane concept a reality. The concept of a CSD can be an integral part of the security screening strategy. CBP's

original plan in December 2003 for a CSD communicated this: "While there will still be spot checks of shipments that raise no red flags, the device serves as a 'sorter,' placing containers into stop-and-go lanes and freeing inspectors to focus on containers that may pose a higher risk."

CSDs hold the promise of providing CBP with information on whether the container was breached between the times it was stuffed and loaded on to a U.S. bound ship. Some CSDs could provide additional data, such as:

- Point of stuffing location
- Identity of person who armed the CSD
- Time that CSD was armed
- Container route information, including transshipment information, as the CSD passes fixed readers

Over the past year, DHS has conducted tests on multiple technologies, from multiple vendors that would be capable of tracking, monitoring, and securing containers against compromise. The Department has been very clear that before incorporating these devices into any government sponsored programs (such as C-TPAT or GreenLane) that the devices must meet a strict 1% false positive threshold. We agree with this requirement. Moreover, policymakers must be careful not to mandate any one technology solution, but rather outline broad requirements of the problem we are trying to solve with CSDs. Technology neutrality is central to fostering competition, innovation, and effective solutions.

Additionally, before incorporating CSDs into the GreenLane, DHS must set standards or issue guidance on the protection of information obtained through these devices. There must also be a cost benefit analysis conducted to ensure that there will be a return on investment, and that these devices will not be cost-prohibitive. Finally, policy and operational requirements for CSDs must be established for these devices so that they can have the confidence of the trade community. Again, to the extent that this legislation focuses DHS to finally make a decision in this critical area, we applaud the Committee's efforts.

Impact on Small and Medium-Sized Businesses

Many existing DHS supply chain security programs are, perhaps unintentionally, designed for large companies that have the economies of scale, internal efficiencies and marketplace leverage to meet demanding requirements. Such large companies employ a "just in time" approach to bringing goods from overseas sources to retail shelves, reducing inventory and costs, while also meeting the demands of consumers. These companies are

therefore both equipped and predisposed to taking the steps necessary to transit the border expeditiously and securely. This then translates into a competitive advantage.

Small and medium-sized companies compete, at a smaller scale, with large companies. They do not, however, enjoy the resources to take costly steps in meeting security requirements. They also do not have the leverage in their buying practices to demand that their supply chain comply with new or extraordinary security measures.

Additionally, small and medium-sized companies employ transportation and other logistics practices that reduce cost, often by pooling those arrangements. An example is their use of non-vessel operating common carriers ("NVOs") to consolidate shipments. These pooled arrangements require different security measures than those utilized by firms shipping in large volumes using full container loads. These small and medium-sized companies are also more likely to use an outside professional, usually a customs broker or freight forwarder, to meet the complexities of moving cargo.

These unique characteristics require that DHS take a more flexible and discrete look at the requirements of small business in the marketplace. DHS needs to acknowledge the differences within the shipping community and permit companies of all sizes to compete on a level playing field.

Moreover, the additional costs that would be imposed by the regulatory compliance framework envisioned in this bill, especially for small businesses, would be steep. Creating more regulatory hurdles for small businesses—such as mandatory "one-size-fits-all" compliance programs—would further obstruct their ability to compete. Congress should bear in mind the staggering cost of additional regulations on small businesses before laying on a heavy yoke of new regulatory requirements:

> *The annual cost of federal regulations in the United States increased to more than $1.1 trillion in 2004. Had every household received a bill for an equal share, each would have owed $10,172, an amount that exceeds what the average American household spent on health care in 2004 (slightly under $9,000). While all citizens and businesses of course pay some portion of these costs, the distribution of the burden of regulations is quite uneven. The portion of regulatory costs that falls initially on businesses was $5,633 per employee in 2004, a 4.1 percent cost increase since 2000 after adjusting for inflation. Small businesses, defined as firms employing fewer than 20 employees, bear the largest burden of federal regulations, as they did in the mid-1990s and in 2000. Small businesses face an annual regulatory cost of $7,647 per employee, which is 45 percent higher than the regulatory cost facing large firms (defined as firms with 500 or more employees)."*

- The Impact of Regulatory Costs on Small Firms by Mark Crain, September 2005.

Third Party Validations

The Chamber opposes the use of third-party validations for C-TPAT members, as both unwise and unnecessary. While we concede that there is a backlog of validations, we believe that the problem has been overstated. According to CBP's own estimates, 66% of all 5,777 certified C-TPAT members are scheduled to be validated by the end of 2006, with validation of 100% of certified members anticipated by the end of 2007. In addition to the 88 supply chain security specialists currently employed to conduct validations, an additional 41 specialists will be employed by the end of summer. We take CBP at its word that these additional resources will allow them to meet their goals. At the same time, we would not object to Congress stepping in and providing additional resources so that CBP can effectively speed the validation process.

In our view, the use of third-party validators differs substantially from simply outsourcing of a government function, which the Chamber typically supports. Such a proposed program, as we understand it, would be tantamount to subjecting companies to external audits. Currently, CBP assigns a supply chain security specialist to each C-TPAT member. These specialists work with the companies directly, gaining a high degree of familiarity with that company's business operations. Moreover, additional questions are raised as to the confidentiality of information collected by potential third parties about business operations and security measures undertaken by C-TPAT companies. We have such concerns about several DHS programs that utilize outside reviews, and to the extent that this legislation highlights this issue, we hope that DHS will take steps to effectively protect such information.

However, if Congress determines that third-parties should be used to conduct validations of C-TPAT members, several issues must first be addressed. First, Congress should require that there is no formal relationship between C-TPAT members and third-party validators. This is necessary to ensure the integrity of the validation process. Second, Congress should recognize that supply chain security validations are unlike other external audits, for the simple reason that supply chain security measures are individually tailored to the needs of each company.

Finally, Congress should answer the fundamental question of who would pay for these audits. Would C-TPAT member companies or the Federal Government bear the cost of conducting these validations? If companies are required to pay for validations, firms may be drawn out of the C-TPAT program. That would, of course, be undesirable.

Office of Cargo Security Policy

Section 5 of the legislation authorizes the creation of an Office of Cargo Security Policy within DHS, headed by a Director. Conceptually, we support the idea of a central point within the Department to coordinate all policy activities related to cargo security. However, we do not see the need for the creation of a new Office of Cargo Security Policy headed by a Director.

We recognize, however, that there is a need for further integration and coordination between all the agencies involved in cargo security. We have long been frustrated by the lack of a central point of contact on cargo security, and have made this point repeatedly to DHS. To the extent that this legislation raises this point more effectively than we have, we appreciate the Committee's support in communicating that message.

Conclusion

In conclusion, the U.S. Chamber of Commerce and our member companies fully support the goal of ensuring the security of maritime supply chains. To the extent that this legislation reinvigorates the policy debate and helps DHS to make long overdue decisions on greenlanes, we congratulate you. However, we remain concerned with a number of provisions in this legislation, especially the regulation of C-TPAT. We would hope that any legislation that originates from this Committee would address the points we have raised with you today.

We look forward to engaging with both the Department and with this Committee to continue effective government programs that further this goal without unduly impairing the flow of commerce. Thank you for providing us with the opportunity to share our views with the Committee on this very important issue. We stand ready to assist the Members of this Committee as you move forward in this effort.