BEST BUSINESS PRACTICES FOR SECURING AMERICA'S BORDERS

HEARING

OF THE

SUBCOMMITTEE ON INFRASTRUCTURE AND BORDER SECURITY

BEFORE THE

SELECT COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

JULY 23, 2003

Serial No. 108–20

Printed for the use of the Select Committee on Homeland Security

Available via the World Wide Web: http://www.access.gpo.gov/congress/house

U.S. GOVERNMENT PRINTING OFFICE
98–523 PDF WASHINGTON : 2005

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) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

SELECT COMMITTEE ON HOMELAND SECURITY

CHRISTOPHER COX, California, Chairman

JENNIFER DUNN, Washington
C.W. BILL YOUNG, Florida
DON YOUNG, Alaska
F. JAMES SENSENBRENNER, JR., Wisconsin
W.J. (BILLY) TAUZIN, Louisiana
DAVID DREIER, California
DUNCAN HUNTER, California
HAROLD ROGERS, Kentucky
SHERWOOD BOEHLERT, New York
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
PORTER J. GOSS, Florida
DAVE CAMP, Michigan
LINCOLN DIAZ-BALART, Florida
BOB GOODLATTE, Virginia
ERNEST J. ISTOOK, Jr., Oklahoma
PETER T. KING, New York
JOHN LINDER, Georgia
JOHN B. SHADEGG, Arizona
MARK E. SOUDER, Indiana
MAC THORNBERRY, Texas
JIM GIBBONS, Nevada
KAY GRANGER, Texas
PETE SESSIONS, Texas
JOHN E. SWEENEY, New York

JIM TURNER, Texas, Ranking Member
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
BARNEY FRANK, Massachusetts
JANE HARMAN, California
BENJAMIN L. CARDIN, Maryland
LOUISE MCINTOSH SLAUGHTER, New York
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ROBERT E. ANDREWS, New Jersey
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
KAREN MCCARTHY, Missouri
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
CHARLES GONZALEZ, Texas
KEN LUCAS, Kentucky
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida

JOHN GANNON, *Chief of Staff*
UTTAM DHILLON, *Chief Counsel and Deputy Staff Director*
DAVID H. SCHANZER, *Democrat Staff Director*
MICHAEL S. TWINCHEK, *Chief Clerk*

SUBCOMMITTEE ON INFRASTRUCTURE AND BORDER SECURITY

DAVE CAMP, Michigan, Chairman

KAY GRANGER, Texas, Vice Chairwoman
JENNIFER DUNN, Washington
DON YOUNG, Alaska
DUNCAN HUNTER, California
LAMAR SMITH, Texas
LINCOLN DIAZ-BALART, Florida
ROBERT W. GOODLATTE, Virginia
ERNEST ISTOOK, Oklahoma
JOHN SHADEGG, Arizona
MARK SOUDER, Indiana
JOHN SWEENEY, New York
CHRISTOPHER COX, California, *ex officio*

LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
BARNEY FRANK, Massachusetts
BENJAMIN L. CARDIN, Maryland
LOUISE MCINTOSH SLAUGHTER, New York
PETER A. DEFAZIO, Oregon
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
CHARLES GONZALEZ, Texas
JIM TURNER, Texas, *ex officio*

CONTENTS

BEST BUSINESS PRACTICES FOR SECURING AMERICA'S BORDERS

WEDNESDAY, JULY 23, 2003

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INFRASTRUCTURE
AND BORDER SECURITY,
SELECT COMMITTEE ON HOMELAND SECURITY,
Washington, D.C.

The subcommittee met, pursuant to call, at 10:30 a.m., in Room 345, Cannon House Office Building, Hon. Dave Camp [chairman of the subcommittee] presiding.

Present: Representatives Camp, Dunn, Granger, Sanchez, Markey, Dicks, Cardin, Slaughter, Jackson-Lee, Pascrell, and Cox, ex officio.

Mr. CAMP. The hearing will come to order. This is a hearing of the Select Committee on Homeland Security, Subcommittee on Infrastructure and Border Security. The subject is Best Business Practices for Securing America's Borders.

I want to thank our witnesses for coming. You may have heard the bells. We have a series of votes that have been called, so I think what we will do—I have been talking to the ranking member, Ms. Sanchez—we will recess the meeting. It may be a little bit of time, but with your patience, we will come back and begin the hearing then. It could be as long as half an hour. There are several votes that are being called.

We will recess the hearing, and be back as soon as we can.

PREPARED OPENING STATEMENT OF THE HONORABLE CHRISTOPHER COX, CHAIRMAN, SELECT COMMITTEE ON THE HOMELAND SECURITY

Good Morning. I would like to thank Subcommittee Chairman Camp, and Ranking Member Ms. Sanchez, for holding this hearing on "Best Business Practices in Securing America's Borders." I am pleased that the subcommittee has taken the time to recognize and discuss this important issue and I look forward to hearing the testimony of the upcoming panel.

Of the myriad challenges facing the Department of Homeland Security, finding a balance between securing our borders from terrorists and allowing the cultural, educational, and financial enrichment that healthy partnerships with other nations provides, is among the most challenging. Historically, one of the United States' greatest assets has been the freedom with which commerce and people have been able to cross our borders. Our policies of the past have helped foster a prosperous and symbiotic relationship with the rest of the world and have helped export the values and message of American democracy.

Unfortunately, the very ease with which people and commerce enter our country puts Americans at risk from those who would wish to harm us. As we found out in the months since September 11th, 13 of the 19 hijackers had entered the United States legally with valid visas. Of the 13, three of the hijackers had remained in the United States long after their visas had expired. This condition highlighted the

systemic weakness of our border security infrastructure and the need to reform the broken system.

Our border security efforts cannot focus solely on preventing would be terrorist from entering the country, but also must keep dangerous materials from being smuggled across our borders. While weapons making their way into the country can be used to carry out attacks against our citizens, the sale of drugs is also a homeland security threat because the profits of those illegal sales can be used to finance other criminal actions such as terrorist groups.

Emerging technology and better business practices are our greatest assets in the fight to improve security without stifling the legitimate flow of people and goods vital to our economy. New technologies are already being utilized to address weaknesses at our borders by screening individuals who seek to enter the country, and managing the information we have about potentially dangerous individuals.

However, it is the job of this Committee and the Department of Homeland Security to seek further improvements and identify best business practices that will continue to improve our nation's security without sacrificing our economic growth or our way of life. I look forward to hearing from our panelists, about how they are working to develop new technologies and procedures that will make our country safer.

Chairman Camp, thank you again for your leadership on this issue and for arranging this important hearing.

Mr. CAMP. The hearing will come to order.

I would like to again welcome and thank everyone for attending today's hearing and apologize for the delay because of the votes.

The Subcommittee on Infrastructure and Border Security will hear testimony from four representatives in the private sector, Mr. Richard Stephens from Boeing, Dr. W. Scott Gould from The O'Gara Company, Captain Houssam Salloum from Axiolog, Inc., And Jeffrey Katz from Atmel.

Your experiences in the private sector and expertise in homeland security technology make your testimony valuable as the subcommittee continues to look at ways to strengthen America's border defenses. Today's hearing will examine the progress being made by the Department of Homeland Security in securing our land and maritime borders, with special focus on efforts to utilize the technology and skill from the private sector. The witnesses will evaluate programs and policies such as the Customs–Trade Partnership Against Terrorism, CTPAT; the Container Security Initiative, CSI; and Fast and Secure Trade, FAST, as well as provide an overview of available technology.

There has never been a more compelling time for our Nation to be educated on the threats and vulnerabilities that terrorists pose to our borders, and how technology can serve as a force multiplier in detecting, deterring and denying potential terrorist activities.

In the post–9/11 environment, guardians of our Nation's borders must plan for a continuous security life cycle. They must recognize security postures can no longer remain static and they must dynamically evolve to meet prevailing threats. As threats change, new vulnerabilities are exposed, and newer mediation programs must be implemented and continually updated.

The United States shares long and large borders with Canada and Mexico, and a very large maritime border of shoreline and navigable waterways. All people and goods legally entering the United States must be processed through an air, land or sea port of entry. An enormous volume of trade also crosses our borders every day. Some 1.35 trillion imports and 1 trillion exports were processed in 2001.

The global trading system is increasingly relying on the swift delivery of goods produced overseas. America's economic stability requires that goods and people cross through our borders and in and out of the country regularly without long delays. Our security also requires that we know who and what is entering.

The Customs-Trade Partnership Against Terrorism was designed to enhance supply chain security. It partners the Bureau of Customs and Border Protection with the trade community to strengthen our borders while facilitating the efficient flow of commerce. Under this initiative, Customs will work with importers, carriers, brokers and other industry sectors, emphasizing the need for a seamless security environment throughout the entire commercial process.

We have a number of initiatives that have been put in place, and I look forward to hearing from our witnesses. I hope we will come away from this hearing with a better understanding of what enhancements can be made to utilize the benefits of the private sector and learn what steps are being taken independently by the security community to strengthen our border defenses.

I now recognize the chairman of the full committee Mr. Cox for any opening statement he may wish to make.

Mr. COX. Mr. Chairman, I thank you for convening this hearing, and Ranking Member Sanchez as well, who I am sure will join us shortly. The votes have just concluded on the floor.

I am very pleased that the subcommittee has taken the time to hear from experts on this important issue. I look forward to hearing from our witnesses this morning. I want to thank you for making time to be with us and bearing with us during an uncertain floor schedule this morning.

Of the many challenges facing the Department of Homeland Security, none is more difficult than resolving the tensions between the simultaneous American goals of security and openness. Following the tragedy of September 11, President Bush stressed the need for America to strengthen our security to prevent another terrorist attack, but he also stressed that we must protect the freedoms that define American democracy, including the freedom to travel and conduct commerce across our borders. We export not only goods and services, but we also export and must continue to export American values. American values bring hope to other people around the world.

Unfortunately, one of our commercial and, if you will, one of our idealistic strengths, the very ease with which we can move about the world and with which people can move into our country, puts Americans at risk from those who would do us harm. As we have learned since September 11, 13 of the 19 hijackers had entered the United States legally with valid visas. Three of those had overstayed their visas substantially; they remained in the United States long after their visas had expired. That condition highlighted the systemic weakness of our border security infrastructure and the need to reform the broken system.

The creation of the Department of Homeland Security was a major step in integrating the Nation's security efforts to improve overall safety by putting all agencies responsible for protecting our homeland under one command with a shared sense of mission. The

former INS, the Border Patrol, Customs and certain elements of the Department of Agriculture merged to form the new Bureau of Customs and Border Protection within DHS.

This merger marked an historic moment. For the first time in our Nation's history, one Federal agency, working hand in hand with the Coast Guard, is now responsible for guarding America's ports and our borders.

While we are focused on our borders today, let me say a few words about our related programs on ports. Prior to September 11, port security involved routine waterborne security patrols and a limited number of container inspections. These were focused mainly on HAZMAT violations. September 11 forced Congress, the Coast Guard, port authorities, State and local officials and the shipping industry to reevaluate.

We have refocused and we have developed programs to improve the way in which our ports are secured. While we still have challenges ahead, we are doing more and better than ever before. The President's Container Security Initiative, for example, deploys Customs and Border Patrol officers to stations overseas. By pushing out our perimeter, we can intercept efforts by terrorists to exploit containerized shipping.

Since the Initiative's launch over a year ago, 20 of the world's megaports have agreed to join CSI and are at various stages of implementation. These megaports, being points of passage for approximately two-thirds of containers shipped to the United States, are vitally important to our security.

While we have a long way to go, we are also making progress on border security, the focus of our meeting today. As Chairman Camp stated, our Nation shares over 5,500 miles of border with Canada and nearly 2,000 miles of border with Mexico. Nearly 500 million people cross the borders into the United States each year. Facilitating the legitimate travel and business for those people is as critical to our way of life as is preventing would-be terrorists from entering the country.

The Bureau of Immigration and Customs Enforcement and the Bureau of Customs and Border Protection have been formed to ensure that these dual missions are rigorously pursued. They are using promising new technologies to facilitate the entry of legal residents and identify those who pose potential threats to our country.

Additionally, the United States is expanding programs and partnerships with the private sector such as the Business Anti–Smuggling Coalition, the Customs–Trade Partnership Against Terrorism and Mexico's Compliant Importer–Exporter Program by developing high tech, dedicated travel lanes which will be made available only to those large firms willing to dedicate extra resources to securing their shipments to the United States.

The Department of Homeland Security also is working with the Department of State on the Visitor and Immigrant Status Indicator Technology, the U.S. VISIT program, at air and sea ports of entry, which is designed to collect information on the arrival and departure of most foreign nationals to determine whether they should be allowed entry into the United States, whether they can change

their immigration status, or whether they have violated their visa status.

Incorporating advanced technologies into our security systems, training our security personnel and using intelligence to target our security efforts are central to the success of protecting our borders. The expansion of current programs and the development of new processes will take time, to be sure, and we must anticipate more bumps in the road; but I am confident that following President Bush's leadership, we will get to our destination of an America safe from terrorism and secure in its freedoms.

I thank our chairman for his commitments and our ranking member for holding this hearing and for summoning these impressive witnesses.

Mr. CAMP. I thank the chairman of the full committee.

The Chair now recognizes Ms. Sanchez, the ranking Democrat member, for any statement she may have.

Ms. SANCHEZ. Thank you, Mr. Chairman.

Obviously, this is the Subcommittee on Infrastructure and Border Security. We have often heard that over 80 percent of the infrastructure that terrorists might be interested in sit in private hands in this country. What we are hoping to hear today from you is some of the technology that we could use and some of the solutions that we might have to protecting that infrastructure.

We recently took a congressional delegation trip, headed by Mr. Cox, out to the Los Angeles–Long Beach area, where we took a look at port security and a nuclear power plant, both things in my area. It becomes pretty evident that we need to be working together because the slowdown, in particular for example, of cargo and container traffic through a large port like L.A.-long Beach, is not only a terrorist problem; but if it should stop, or as we try to protect physically some of this cargo or protect ourselves, we may slow down the process of moving cargo through these ports and across our Nation. And, of course, that has a great economic impact.

In fact, I was recently over at the defense college here in the area, and we worked on that port scenario in particular, to take a look at what it would like look if we closed down traffic in some of our major ports. And being from the L.A.-long Beach area, one of the things that we saw in the lockout in the port area was not just all of the container freight sitting right off our coast all of the way down through Orange County, but more importantly, the significant impact of almost $20 billion worth of economic impact or loss to our Nation.

Just because it is in Los Angeles and Long Beach does not mean that it does not affect the rest of the Nation, because that cargo and those sales are done throughout the Nation. I have met with some of you before, and I am excited that our members here will get to see some of your technology and see some of the solutions as we try to find a quicker and good way to find a fix, and a smart way.

Mr. CAMP. The Chair now recognizes Representative Dunn for an opening statement.

Ms. DUNN. I look forward to hearing from our witnesses today. The issue is a very important one to my constituents in Washington State and, in particular, to the Seattle area which faces a

unique set of security challenges. The international border and the coastline, as well as the presence of international companies, such as Boeing and Microsoft, make my home a particularly vulnerable place.

Washington State thrives on the commerce created by trade across our borders. The State's tourism industry depends on travel across our northern border. The cruise line industry is quickly becoming a major and welcome presence in Seattle. Therefore, any changes in the exchange process affect our economy and, therefore, my constituents.

Our security, whether it be in the cyberworld or at our seaports and international borders, depends on public-private relationships; and so today, our committee is here to learn about the technology that our private sector partners are developing to make our borders and ports more secure. This Nation's private companies have been responsible for great technological innovation, innovation which has allowed us to make great strides in our security efforts already.

I am aware of the technological developments happening at Boeing in the area of baggage screening. And Mr. Stephens has been a lead voice in an aviation security study project, which has involved industry stakeholders; and I look forward to finding out a little bit more about that during the questioning period.

We will continue to rely on private companies and support them while they continue to develop new technology. I look forward to your testimony.

Thank you, Mr. Chairman.

Mr. CAMP. Without objection, any member may place an opening statement in the record, or revise and extend their opening statement.

Again, I would like to thank and recognize our panel for the testimony they are about to offer, Mr. Richard Stephens from Boeing, Dr. W. Scott Gould from The O'Gara Company, Captain Houssam Salloum from Axiolog, Inc., And Jeffrey Katz from Atmel.

We have received your written testimony. You may summarize your statement in 5 minutes. We will start with Mr. Stephens.

STATEMENT OF RICHARD STEPHENS, VICE PRESIDENT AND GENERAL MANAGER, HOMELAND SECURITY AND SERVICES, THE BOEING COMPANY

Mr. STEPHENS. Mr. Chairman, and members of the subcommittee, thank you. I appreciate the opportunity to appear before you today to discuss best practices as they relate to homeland security and, particularly, border security.

As you are aware, one of the biggest challenges that we face as a global community is defining the respective roles governments and business leaders play in the war on terrorism. Collectively, our jobs are to find ways to stop terrorism so that people feel safe and to protect the means that support our global economic prosperity. This is a large and complex problem. The approach must be complete and integrated if we are to find a comprehensive and efficient solution to this clear and present danger.

Clearly, terrorists are strategists. They choose their targets deliberately. They know no boundaries and operate within and outside our borders, as was evidenced on 9/11.

We have to catch them before they act. To do that, we must augment and integrate the best information and management systems possible to collect information and connect the dots in time to thwart any attack. We need to see, to know, and to understand. We must anticipate the security challenges on all fronts.

As the world's largest aerospace company, Boeing has developed many best practices for developing and implementing large-scale solutions to issues that require the interaction of people, processes, and technology. The skills we have developed by integrating advanced systems for defense, space, intelligence, homeland security, and commercial customers are directly applicable to solving the large, complex problems the United States faces in homeland security.

Based on our experience, we identified the following seven proven tenets that apply to successful, large-scale integration projects. We offer them as best practices that can be applied to homeland security and could help increase the security of our Nation's borders.

The first is to create partnerships with the customer and key stakeholders and align the expectations of all the parties.

Second is to leverage large-scale systems integration and network centric operation capabilities to meet market and our customer needs.

The third is fundamentally important and that is to partner and align with the best-in-class companies.

Fourth is to develop standards that provide open architecture solutions, so any technologies made available can, in fact, be brought to continue to improve and enhance the systems put in place.

The fifth one is also important, because we are talking about the expenditure of not only business resources, but government resources; and that is to conduct modeling and simulation and operation analysis to make sure we shape the solutions before we implement them.

Sixth is identifying risks early and use solid risk management plans to make sure that the solutions we are talking about are on time and meet the objectives.

Last on the list is to share information real-time with all of the customers, the stakeholders and partners.

I have used the term "customer" a number of times and believe it is important to emphasize that, ultimately, the customer is the American public, the business community, and the government infrastructure that supports our democracy.

Aviation and border security face similar challenges. Let me give an example how we applied these best practices to the airport and aviation security last year when the government selected Boeing to help Americans feel secure about air travel by supporting the Transportation Security Administration in meeting a congressional mandate to screen 100 percent of checked bags by December 31 of this last year at all of our Nation's commercial airports.

Many experts thought the job was not possible, but we accomplished that goal by building a world-class team and working hand in hand with our customers, which included the Transportation Security Administration and the aviation industry. We applied our expertise and proven principles as a lead systems integrator, and

in 207 days the Boeing team conducted site surveys, did preliminary designs, did final designs, did facility modifications, installed more than 6,000 explosive detection systems and explosive trace devices at over 400 commercial airports in the United States, and trained more than 25,000 checked-bag screeners.

The TSA-led efforts to secure America's airports employed many of these tenets that I talked about, and most important was the first one, and that was to ensure we had all of the stakeholders pulled together. Over 3,000 stakeholders were involved nationwide, including the Nation's airports, the airlines and many other officials at the State and local levels.

Using tenets 2 and 3, we drew on the expertise from across the company and our supplier partners. We grew from a core of 100 people to over 30,000 strong, working together with the aviation industry to achieve the goal of 100 percent baggage screening. While most would agree that there was some additional work to be done to smooth out the rough spots in the system, given the time and resource constraints, the job was accomplished well and America's aviation system is much more secure.

We are now leveraging the work we did and the lessons learned to support additional homeland security large-scale systems integration opportunities, where again we have complex goals and complex challenges. As you are aware, Boeing and its best-of-class partners were selected for one of the Operation Safe Commerce programs, specifically to work the Los Angeles and Long Beach area, and will be conducting similar demonstrations at other seaports around the U.S. We are using all seven tenets I described above.

Within the Boeing company, we recently initiated an Integrated Border Awareness and Management study to understand how the U.S. border operates, including its stakeholders, processes, and technologies. Because Boeing is, in fact, the Nation's largest exporter, with business sites located at significant borders of entry, Boeing has a vested interest, as well as obligation, to use its people, processes and technology towards improving security at U.S. borders. We also have a vested interest because we need to ensure our global customers are able to gain entrance to the United States to train their pilots and aircrews to be able to operate our particular products.

That having been said, we are not necessarily experts on border security. However, we recognize the challenges that are faced in the border area, including large, complex management challenges with multiple legacy systems, little or no intraoperability or communications capability, difficult or impossible-to-access information to make decisions, and situational awareness and tactical information being undefined.

Congress has mandated the U.S. VISIT program to address some of these near-term security issues. Our company, along with many others, is looking at long-term solutions, and we recognize the importance of including U.S. VISIT as the first phase. However, we also encourage the government to be sensitive to defining requirements in such a way that it does not stifle the inventiveness that industry can bring to the table.

Border security also requires large-scale integration of information gathering and multiple layers, similar to what was developed for the aviation industry. Looking back to the enormity of the aviation security project, we cannot afford gaps in the system.

Six Sigma, which became a watchword for quality control in the 1980s and 1990s to help enhance manufacturing production by measuring defects in parts per million simply is not good enough when we are talking about the Nation's security. As such, as we look at trends, we believe there needs to be a multilayered approach to ensure that any potential breaches in the system are picked up by other layers.

Border security is a hard job. Many organizations are involved, and there is a lot of sharing of information that must take place in ways that we have never shared information before. Many varied stakeholders must work together protecting not only America, but also the resources that make our economy strong and vibrant. Very few companies have the ability to integrate systems at the scale we are talking about for U.S. borders.

For any integration to be successful, there must be partnerships between the government and industry, and both must follow the best practices that I mentioned previously in my statement. We have available, if you would like, a document we call "All Systems Go." It is a document we use on a regular basis to share with our customers and constituents some of the tools we use on a regular basis, and we are pleased to share that with you.

That concludes my statement and I will be pleased to answer any questions you have, Mr. Chairman, or members of the committee have.

Mr. CAMP. Thank you very much.

[The statement of Mr. Stephens follows:]

PREPARED STATEMENT OF RICHARD STEPHENS

Mr. Chairman and Members of the Subcommittee:

Good Morning. I am Rick Stephens, Vice President and General Manager of Homeland Security and Services for The Boeing Company. I appreciate the opportunity to appear before you today to discuss best business practices as they relate to border security.

One of the biggest challenges we face as a global community is defining the respective roles world governments and business leaders will play in the war on terrorism. Collectively, our jobs are to find ways to stop terrorism so that people feel safe and to protect the means that support our global economic prosperity. This is a large and complex problem. The approach must be complete and integrated if we want to find a comprehensive and efficient solution to this clear and present danger.

Terrorists are strategists. They choose their targets deliberately. We have to catch them before they act. To do that, we must augment and integrate the best information and management systems possible to collect information and "connect the dots" in time to thwart any attack. We need to see—to know—and to understand. And to do that we must be vigilant. We must anticipate security challenges on all fronts.

As the world's largest aerospace company, Boeing has developed many "best practices" for developing and implementing large-scale solutions to issues that require the interaction of people, processes and technology. The skills we have developed by integrating advanced systems for defense, intelligence and commercial customers are directly applicable to solving large, complex problems the United States faces in its homeland security mission.

Based on our experience, we identified the following key principles that apply to successful large-systems integration projects. We offer them as best business practices that can be applied to homeland security and could help increase the security of our nation's borders:

- Create partnerships with the customer and key stakeholders and align expectations.

- Leverage large-system integration and network centric operations capabilities to meet market and customer needs.
- Partner and align with the best-of-class companies.
- Support development of standards that provide open architecture solutions.
- Conduct modeling, simulations and operational analysis to help shape the way forward.
- Identify risks early and use solid risk management plans.
- Share information real-time with the customer, stakeholders and partners.

Let me give you an example of how we applied best practices to the airport security program. Last year, the government selected Boeing to accomplish what many considered an impossible job—help Americans feel secure about air travel by meeting a Congressional mandate to screen 100 percent of checked baggage by Dec. 31, 2002 at all the nation's commercial airports. Many experts thought the job was not possible. But we accomplished that goal by building a world-class team and working hand-in-hand with our customer, the Transportation Security Administration and the aviation industry.

We applied our experience and business principles of lead systems integration to the airport security project. In less than six months, the Boeing team installed more than 6,000 explosive detection systems and explosive trace devices at 439 commercial airports in the United States. The Boeing team also trained more than 25,000 checked baggage screeners. This represents one of the largest short-term projects in U.S. government history.

To reach the objective, we needed the involvement and buy-in of more than 3,000 stakeholders nationwide—TSA (now a part of the Department of Homeland Security), the nation's airports and airlines and many other officials at the state and local levels. The Boeing program team, drawing on expertise from across the company and its supplier partners, grew from a core group of 100 to more than 30,000 strong, working together with the aviation industry and government stakeholders to achieve the stated goal of 100 percent baggage screening. While most would agree that there is additional work to be done to smooth out the rough spots, given the time and resources constraints, the job was accomplished and America's aviation system is more secure.

We are now leveraging the work we did with the airport security program to support additional homeland security large-scale systems integration opportunities where meeting extremely complex goals with the greatest possible urgency and efficiency to help keep Americans safe and secure is required. As you are aware, Boeing and its best-of-class partners were selected for one of the Operation Safe Commerce programs. We are working directly with the stakeholders involved in examining, securing and tracking goods shipped into the ports of Los Angeles and Long Beach and we will be conducting similar demonstrations at other seaport locations.

Within the Boeing Company, we recently initiated the Integrated Border Awareness and Management (IBAM) study to understand how the U.S. border operates, including its stakeholders, processes and technologies. Because Boeing is the United States' largest exporter with business sites located near significant border ports of entry, Boeing has a vested interest -- as well as an obligation -- to use its people and technologies toward improving the security at U.S. borders.

That said, we are not experts on border security. However, we recognize the challenge the federal government faces in securing our borders—7,500-plus miles of border with Canada and Mexico, 95,000 miles of shoreline and navigable waterways, 300 ports of entry. Our initial study of current border management helped us recognize the environment we were dealing with:

- Large complex management challenges with multiple legacy systems and organizations;
- Little or no interoperability or intercommunication capability among the managing agencies;
- Difficult or impossible-to-access information to make decisions is unavailable at the front line;
- Situational awareness and tactical information undefined, for example, where problems are occurring, where resources are located, how to make the best deployment/intercept choice, and how to efficiently and accurately determine the status of a person, cargo or vessel.

Congress has mandated the U.S. Visit program to address some of these near-term security issues at the borders. Our company, along with many others, is looking at long-term solutions and we recognize the need to incorporate U.S. Visit as a first phase. We encourage government to be open in its requirements so not to stifle the inventiveness of what industry can bring to the table.

But border security also requires a large-scale integration solution utilizing information-gathering tools and technology, modeling and simulation, and network cen-

tric operations in a layered approach similar to what the Transportation Security Administration developed for airport security.

Looking back to the enormity of the challenge of the aviation security project, we can't afford gaps in the system. Six Sigma, a key quality control concept in the 1980s and '90s that enhanced manufacturing production by measuring defective parts per million, simply isn't good enough when you're talking about the nation's security. We are reviewing information occurring in millions of transactions per day, looking at trends and political issues and, as some would say, moving the haystacks away so we are left with the needles.

Network centric operations gathers those millions of pieces of information and delivers them in such a manner as to give a common operating picture. This helps decision makers manage risk by getting the right information to the right people who have to act on it at the right time. We must have a layered approach to make sure that there are no gaps in the system. In aviation security, those gaps in information are covered by checking passengers, screening baggage, reinforcing cockpit doors and using federal air marshals.

A network centric environment is about creating the systems and capabilities that allow us to understand the situation with speed, accuracy and efficiency. It's about integrating communications and information systems that provide insight into the status of security from airplanes to airports, from cargo to passengers. It's also about interlinking data on shipping container information, cargo status and manifest into a centralized global database. And it's about using sensors to gather data, integrate it and correlate it in order to create an integrated awareness of the situation so that key decisions can be reached and actions taken.

Right now, we have software intelligent agents that can pull that information together in a matter of minutes, presenting authorities with a threat correlation report and probability of a plausible terrorist plot. They look for the common thread -- like shared phone numbers, credit card and drivers license numbers, flight data, etc. Software intelligent agents act like a continually running search engine. In fact, you don't have to tell the search engine to go find the information—it does it for you. It anticipates your needs based on knowing your requirements. In this way, the network becomes our best arsenal in the war on terrorism

Conclusion

Global security isn't about being reactive—it's about being proactive. In order to be proactive, we must have information at our fingertips at all times, continually investigating before the fact.

I believe border security requires the information superiority vision of tomorrow. And our industry, companies like Boeing and others, is responding to the call to duty. In the future, systems will give us all the information we need. But until we tie these systems together and they talk to each other, we're still vulnerable. We need knowledge to move forward. And a network centric environment gives us that knowledge.

Border security is a hard job. Many organizations are involved and there is a lot of sharing of information that must take place in ways that we have never shared information before. Many varied stakeholders must work together to protect not only America but also the resources that make our economy strong and vibrant.

Very few companies have the ability to integrate systems at the scale we are talking about for U.S. borders. For any integration to be successful, there must be a partnership between government and industry and both must follow the best business practices that I mentioned previously in my statement.

That concludes my statement, Mr. Chairman. I would be pleased to address any questions you and other members of the subcommittee might have.

Mr. CAMP. Captain Salloum.

STATEMENT OF CAPTAIN HOUSSAM SALLOUM, PRESIDENT AND CEO, AXIOLOG

Mr. SALLOUM. Mr. Chairman, honorable members, I thank you for this opportunity to speak before this committee.

Homeland security has dual challenges to make sure that our borders are protected and, at the same time, to make sure that the flow of the cargo goes smoothly to the ports. I would like to leave you with three main bullets, if I may, today.

The first thing I would like to suggest is efficiency and security must go hand in hand from a commercial perspective. If we empha-

size efficiency, efficiency by itself could compromise security; and if we emphasize only security, security could choke the economy. So they must go hand in hand.

To really have security, we must think globally. With global visibility, we need to know what this warehouse is moving, what cargo around the world, in order for us to flag that particular shipment. So I need to know if this particular warehouse is moving cargo from, for example, Yugoslavia, coming to our country, what this particular warehouse imports; whether he has been involved in any suspicious activity, and is this the first time he has moved cargo to our country? So this is important for our security, to protect our borders, we must have global visibility.

In order to have and achieve the global visibility, we must provide commercial benefits to the global logistics industry, and definitely that can be achieved by considering the commercial benefit that the system must provide to the global logistics industry.

I would like to draw your attention, Mr. Chairman and members, to the second slide that I provided. We believe it is a very simple approach. Global cargo security must combine efficiency and security, and to achieve efficiency and security, global visibility is a must. And to do that, commercial benefit is the key to achieve this.

Also I have included a slide, the last page in our handout, to give an idea of the flow of the shipment coming from overseas. So, in other words, we have here a foreign warehouse, we need to know about the activity of this warehouse, and his import and export activity, and this is the intelligence part of our security.

Once the shipment is on the move to our country, we need to provide information to the Coast Guard so they can stop that ship or plane or that truck before getting to our country. That is before getting to our country. Once this happens, the same system must provide information to Customs so they can decide to flag the suspicious shipment or the suspicious enterprise. Because this is what is needed: We need global visibility, global data history, we need to apply true monitor lists, which is the Enterprise Monitor List and Shipment Monitor List, in order for us to flag a suspicious shipment.

Once we achieve that, a few things have to be talked about the cargo when it is already in our country. Who is making sure that this container at the port is going to the warehouse where it has been manifested? The same system must be able to create some kind of geographic analysis of the movement of the truck from the port all of the way to the warehouse. So, if this truck, for example, goes to a different warehouse, an automatic signal will be sent to the local security enforcement officials to stop that truck, or at least go to this particular warehouse where the shipment has been discharged.

In other words, we believe that the system must definitely be global—we need to have global participation. This is why also, when we visited Europe and we met with the cargo officials there, they liked very much the strategy that we have discussed; and they said we were consistent with their vision, because they also believe that commercial benefits is a key element to have a global participation in this cargo security system. So everybody will not fax a bill of lading or will not fax the shipment manifest; rather, they

will feed in this data so we can have a record and a single source system that will give us the information we need to flag a suspicious shipment or suspicious enterprise.

Thank you, Mr. Chairman.

[The statement of Mr. Salloum follows:]

PREPARED STATEMENT OF CAPTAIN HOUSSAM SALLOUM

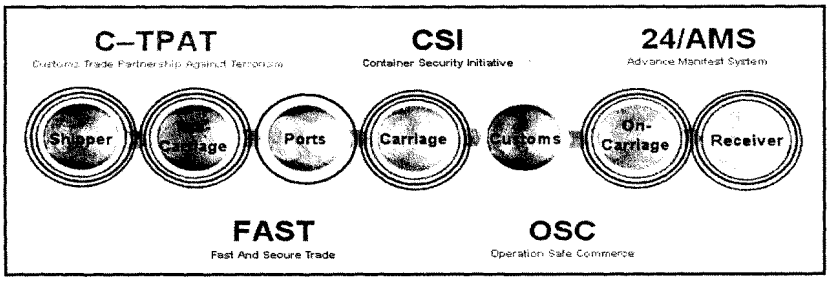
Introduction

The leadership of the U.S. Department of Homeland Security in developing plans to protect our borders is to be commended. This department through the Customs & Border Protection has the extremely demanding "dual challenge of protecting our citizens and our borders from terrorists and the implements of terror, while facilitating the flow of legitimate trade."

Following September 11, 2001 multiple Homeland Security programs have been launched to protect our borders from terrorist incursions via commercial shipments. These programs include Operation Safe Commerce (OSC), The Container Security Initiative (CSI), Customs Trade Partnership Against Terrorism (C–TPAT), and the Advance Manifest System (AMS).

These initiatives have been created to address specific subsets of shipments. In essence, the flow of a shipment has been broken down by tasks. This is due to the fragmented nature of international shipping. To illustrate, a relatively simple lane from a GM Silao assembly plant in Mexico to dealerships in Jacksonville, Florida involves 19 shipping events with 11 different companies, each employing their own proprietary information management systems. In global lanes, transshipments and consolidations can significantly increase the number of events and participating organizations.

For years, the global shipping industry has been seeking new methods to integrate these participants in order to improve efficiency and boost profits. Yet, no end-to-end system to manage this industry exists today. Given this reality, the U.S. Department of Homeland Security had little choice but to concentrate enforcement efforts on specific entities. This has led to overlaps. For instance, one shipment may be impacted by five different initiatives from the Customs & Border Protection alone. Any given entity may also be impacted by multiple initiatives.



(Figure 1)

As shown above, shippers/receivers, carriers, and intermediaries are invited to join C–TPAT and FAST. While CSI is designed for ports program may impact nearly every entity involved in shipping. Likewise, under the "24-hour" rule carriers electronically file manifest information. Nevertheless, this rule affects all shipping participants, since this information is supplied by shippers and may delay delivery if it is not presented properly. Since these overlaps involve only one government agency and these programs already lead to concerns amongst shipping participants, they may wonder about the following:

- What sort of overlaps will exist once the Office of Homeland Security becomes fully operational?
- What sort of overlaps will exist when international governments and the World Customs Organization introduce their own cargo security rules?
- Why is there no coordinated, global approach to cargo security?

Combining Efficiency and Security

The global economy demands efficient and secure global logistics. For any security system to be embraced worldwide, it must include commercial benefits. In other words, efficiency and security must go hand in hand. Efficiency by itself may com-

promise security. In contrast, overarching cargo security rules and regulations could damage the economy. Therefore, a comprehensive public/private sector solution must be implemented in order to economically and effectively deal with cargo security challenges. To encourage maximum private-sector involvement, the overall solution must deliver commercial benefits.

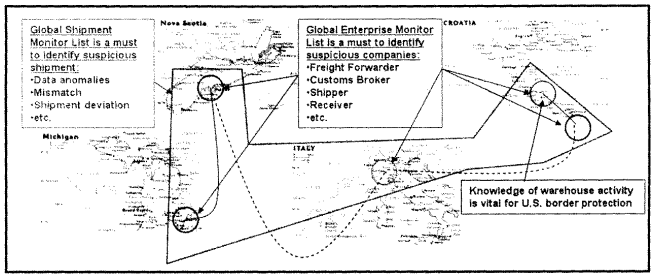
As an illustration, consider sea ports. Ports around the world are now being squeezed by seemingly opposing forces.

- Requirements of security initiatives to provide for more inspections, and improve the security of facilities.
- Pressures from shippers and carriers to process cargo faster and more efficiently.
- Real business needs to contain costs and improve profitability.

Failing to accommodate all of these forces will lead to imbalances that may result in financial losses, delays in the processing of cargo, and/or compromised security. None of these developments is acceptable.

We assert that to effectively address cargo security whether domestically or internationally, a holistic system must be enabled that takes the entire flow of global shipments into account, from the empty container in a depot to the final receiver. Such a comprehensive approach must strive to meet two core objectives; 1) Encourage widespread private sector involvement by improving the process efficiency and profitability of all parties involved in shipment flows, and 2) Deliver cargo security improvements from the private sector that complement and reinforce official rules and regulations.

Cargo Security Guidelines Require Global Visibility



(Figure 2)

Suggested cargo security guidelines include;

- To be proactive, U.S. Homeland Security agencies must collect real-time global shipping activity data and apply sophisticated artificial intelligence in order to identify and flag suspicious shipments, regardless of port or country of origin.
- When addressing U.S. national security, it is crucial to cross-check data from official sources with private sector data to test for integrity and consistency.
- U.S. national security should not depend on the integrity or capability of a single source of information or individual data sources in foreign countries.
- Limitations in technology capabilities in foreign countries should not hinder the flow of timely quality data from any foreign country.
- Despite any political or cultural differences, U.S. agencies should be able to receive reliable data from foreign countries.

Cargo Security Initiatives Enhancement

Keeping the above guidelines in mind, let us now consider how the following three primary Customs & Border Protection initiatives can be enhanced; the Customs Trade Partnership Against Terrorism, the "24-hour" rule, and the Container Security Initiative.

Customs Trade Partnership Against Terrorism

C–TPAT is the Customs Trade Partnership Against Terrorism. This private/public sector partnership involves Customs inviting private companies involved in the flow of a shipment, from shipper to receiver, to help improve international supply chain security by applying "best practices" for security to their organizations.

Issues

C–TPAT is a good concept and the underlying ideas of voluntary "best practices" programs to improve supply chain security are reasonable. Yet, officials within homeland security have stated that mandates will be required in order to truly im-

prove cargo security on the large scale. New cargo security legislation and advanced manifest laws provides previews of mandates to come.

On the global scale, corporate shipments are vulnerable based upon the realities of international shipping. C–TPAT members may have the most secure organizations, contract only secure suppliers, and utilize secure intermediaries and still have their shipments delayed or hijacked based upon the following reasons:

- C–TPAT cargo mixes with less secure cargo on the same vessel.
- Corporate shipments may be used by terrorists as a cover-up for their activities.

To address these issues, a comprehensive security system should be enabled that addresses high-volume and low-volume shipper's shipments as well.

The top twenty-eight ocean container carriers represent approximately eighty percent of the global movement of sea containers. Therefore, by establishing twenty-eight secure data connections, the majority of global shipping data will be accessible. Applying artificial intelligence to this commercial data and establishing two monitor lists, Enterprise Monitor List (EML) and Shipment Monitor List (SML), will enable new capabilities to flag suspicious enterprises involved with a given shipment and/or a suspicious shipment itself.

Shipments will be monitored for data mismatches, data anomalies and shipment flow deviations. In other words, through integration with corporate shipper supply chain management systems, the SML will identify the responsible parties who load, survey and move shipments throughout global supply chains. In addition, the system will know how long various events should take and how long they actually took (forecast vs. actual). This capability will be enabled by the process of combining global events with satellite tracking.

This approach has been independently validated by other organizations that recognize the strengths of enhancing official programs with private sector initiatives. In its recent *Cargo Security White Paper* the National Customs Brokers and Forwarders Assoc. of America, Inc. (NCBFAA) outlined some ideas to enhance C–TPAT and cargo security. In particular, they summarized a "Chain of Custody Dataset" or CCD. The CCD looks very much like the EML and SML approach. According to the NCBFAA, the CCD ". . . will provide the deep penetration into supply chain risk evaluation that is necessary to detect security risks from the remotest source to the final receiver."

The Advance Manifest System

The "24-hour" rule states that ocean carriers must electronically submit completed shipment manifest information to Customs & Border Protection, via their Automated Manifest System, 24-hours prior to loading vessels bound for U.S. ports. As of December 2, 2002, Customs & Border Protection made this rule mandatory. This rule has also become law under the Port and Maritime Security Act of 2001 (S.1214). Effective October 21, 2003 this law will be expanded to include truck, rail, and air. Reporting times vary by mode. For instance, the interim ruling states that truck carriers must submit their electronic manifest information from 30 minutes to 1 hour before they arrive at U.S. border crossings.

By far the most controversial law designed to address cargo security is the "24-hour" rule. There has been considerable resistance from the private sector to the "24-hour" rule. For example, in extensive comments to Customs & Border Protection concerning this matter, World Shipping Council President Christopher Koch articulated several industry concerns with this plan. Mr. Koch and the forty-plus ocean carriers he represents have expressed concerns about potential negative impacts the "24-hour" rule may have on their businesses.

Issues

There are also several security and operational problems associated with the overemphasis on shipment manifest information in existing cargo security plans. The shipment manifest was never intended to be an informational resource for cargo security. The shipment manifest is the sum of bill of ladings associated with a vessel/voyage. It is noteworthy that the shipment manifest is a key component of S.1214 which "requires ships to electronically send their cargo manifests to a port before gaining clearance to enter, and prohibits the unloading of improperly documented cargo."

The ultimate sources of manifest information are the shippers. In essence, the system is relying upon shippers to be honest about what they are shipping. And when certain officials were asked how they would confirm that manifests are filled out correctly, they proposed to ask the freight-forwarder. This begs the following questions;

- How will the freight forwarder actually know what was in a container?

- How effective is any process for identifying suspect shipments that relies on shipment manifest information self-reported by shippers?

Since freight-forwarders only charge nominal fees to submit bill of lading instructions on behalf of shippers, they can not afford to physically inspect shipments. Therefore, freight forwarders do not actually know what is in a container. The only person who actually knows what is in a container is the shipper. In essence, there are two principal issues associated with relying on shippers to provide information used to screen their own shipments.

- How can government agencies be certain of any given shipper's integrity?
- Even when a shipper is reliable, can his or her shipment still be hijacked by terrorists?

Once again, enabling EML and SML capabilities will help to confirm or deny the integrity of shippers and/or shipments on the global scale. Intelligently analyzing historical private sector shipping data concerning large and small participants involved in a shipment and introducing real-time monitoring of shipment data will help address the issues outlined above. In addition, incorporating the systems of land, air, and/or ocean carriers will provide up-to-date information about the actual movements of the international freight of corporate and individual shippers.

The Container Security Initiative

CSI is the Customs & Border Protection Container Security Initiative. The idea behind CSI is "pushing back the borders" to the port of origin. This plan involves stationing Customs & Border Protection inspectors in foreign ports to assist the prescreening of containers bound for the US. Initially, the top twenty mega-ports, representing "roughly 68 percent of the 5.7 million sea containers entering the U.S. annually" were invited to join CSI.

Issues

Due to the nature of the shipping business, ships that are employed on regular service typically call on about eight ports per voyage on average. Therefore, their itineraries are not limited to mega-ports. The common links between these ports is the vessel. A given port could invest large amounts of resources to address the security of cargo moving through that port, and yet a ship sailing from this secure port could be denied entry into a U.S. port due to suspicious containers that were loaded at smaller ports that are not part of CSI.

Additional political and economic factors have emerged that bring the present design of CSI into question. For some time, U.S. ports have been concerned that the "24-hour" rule may provide a competitive advantage for Canadian ports. This is due to the fact that shipments being unloaded in Canadian ports, ultimately bound for the U.S. via road or rail, are not subject to the "24-hour" rule. U.S. ports have legitimate concerns that cargo may be diverted from U.S. to Canadian ports as a result. Another perspective on CSI came to light in a *NY Times News Service* article *Port Security Plan Irks Europeans (11/6/02).* According to this report, "European Union officials are concerned that the program's incentives favor those ports that sign the agreements and penalize those that either refuse or are too small to take part." Likely, cargo that has been pre-screened at CSI ports will be subject to less rigorous inspection at U.S. ports than non-CSI shipments. EU officials state "that companies shipping goods to the United States will start rerouting their cargo to ports like Rotterdam, depriving others of business and potentially creating bottlenecks in some shipping regions." As if to drive home this point, 'A Dutch customs official *(stated)* the U.S. agreement was not just a way to prevent terrorist attacks. "It's good for business," she said.' The EU views European Customs agreements as European Community agreements. Therefore, "the EU is considering the possibility of beginning infringement procedures against countries that have signed on to the initiative." Even though a compromise was reached to avoid this suit, it points out how cargo security rules may have unintended consequences.

Since the common denominator regarding international ocean freight movements are ships, not ports, methods to confirm the integrity of containers aboard ships must be put into action. Incorporating vessel specific information into the EML and SML system will improve the intelligent screening of cargo at any port and terminal. When integrated into port security and customs operations, this approach will improve the targeting of cargo for scanning or inspection by customs officials. This technique will help address the competitive and operational issues associated with the present design of CSI. Significantly, this approach has been recognized by top officials within U.S. Homeland Security Departments as "ahead of the game."

Commercial Benefits

Any commercially viable e-logistics network should be designed to standardize and simplify shipping processes for shipping participants. It should offer smart business

tools to enhance the reliability and dependability of logistics by bringing shippers and carriers closer together, helping organize the private shipping market, and improving logistics providers' service delivery. Increased costs of enhancing cargo security should be offset by a system that provides economic benefits. Following are key benefits such a system should deliver for members of the global shipping community.

Carriers:

- Unique tools for managing capacity utilization and minimizing dead space.
- Organizing the private shipping market.
- Minimizing non-value-added activities between shippers and carriers, increasing carrier and shipper ROI.
- Enhancing relationships with contracted corporate shippers via integration into global supply chain management systems.
- Compliance with new and emerging international governmental cargo security regulations.

High-Volume Shippers:

- Integrating Just-In-Time Inventory with JIT Shipping.
- Global Coverage and Tracking.
- Global Visibility (status, freight costs, survey).
- Global Documentation and Claim Processing.
- Automated Exception Processing.
- End-to-End Real Time Performance Monitoring.
- Compliance with new and emerging international governmental cargo security regulations.

- Low-Volume Shippers:
- Allowing shippers to evaluate and select carriers serving desired destinations, based upon individual shipment needs.
- Allowing shippers to obtain real-time rate quotes, complete bookings, and submit bills of lading online.
- Providing shippers with access to information concerning customs, insurance, financing, and warehousing, etc.
- Providing, for example, an Italian shipper moving cargo from Brazil to South Africa, with door-to-door shipment to obtain personalized service provided through the selected carrier's local agent networks.
- Standardizing and expediting claims processes.
- Standardizing and expediting documentation processes.
- Delivering global coverage using multiple carriers and multiple modes of transport.
- Enabling real-time global tracking by combining GPS and/or RFID with event status reports.

Ports:

- Cost effective means to target suspect shipments for inspection prior to loading.
- Cost effective means to target suspect shipments entering the home country.
- Providing smart tools to help plan and maximize port capacity utilization.

Delivering commercial benefits for all participants in global logistics must be the basis of any security system. This approach will place that system in a distinctive position of helping to enhance cargo security, while improving the efficiency of private companies' global logistics networks.

Conclusion

The required technology should provide proactive information to multiple security agencies. Let's take as example a containers coming to the United States by ship. **Intelligence Agencies:** The system must provide intelligence to the intelligent agencies about the warehouse activities overseas. **Coast Guard:** On board ship and now six miles from the U.S. port of entry, proactive information is made available to the United States Coast Guard on the contents of the ship, and what's in the containers. The Coast Guard now knows the immediate history of the ship and its cargo. Any suspicion results in stopping the ship while it is still in international waters. **Customs:** At the ports, the US Customs agents are given all information necessary to flag suspicious shipments or enterprises. But the information flow doesn't end here. **FBI/State police / Local law enforcement:** When the freight/goods leave the port of entry for an in-country delivery or drop off, the system will automatically track each shipment. Any time the shipment deviates a signal will be sent automatically to local enforcement officers. This is necessary and now possible for domestic security.

In order to tackle the significant potential threats posed by the massive volumes of domestic and international cargo shipments, any solution must be commercially viable and be able to rapidly scale to handle high transaction volumes. Such a global solution must also provide methods to include every entity involved in the global shipping industry (land, air, and sea) into a cohesive cargo security strategy. To encourage maximum private-sector involvement, the overall solution must provide clear commercial benefits.

Axiolog appreciates being invited to address this committee, and looks forward to assisting your continued efforts in protecting America's borders.

STATEMENT OF W. SCOTT GOULD, THE O'GARA COMPANY

Mr. GOULD. Mr. Chairman, thank you for inviting me here today to participate in the discussion about Best Business Practices for Securing America's Borders.

The previous witnesses and Mr. Katz have focused their remarks on specific kinds of systems and technologies that could secure our land borders and other ports of entry and prevent the entry of terrorists and weapons of mass destruction to our shores. I will focus my remarks in a different, but equally important direction, specifically on the best practices that government can utilize to ensure that it makes appropriate and beneficial investments in homeland security systemwide. These best practices are an application of portfolio investment techniques and the creation of common and open standards for technology purchased through the Federal procurement system.

Recently, my company, The O'Gara Company, published a report on these and related topics entitled "The Homeland Security Market: Corporate and Investment Strategies for the Domestic War Against Terrorism." I have copies of that for Members and staff. Key excerpts from this report can be found at the end of my written testimony. My co-author, Chris Beckner, and I would be happy to make full copies of the report available after the hearing.

Making appropriate investment decisions and allocating resources in alignment with the threats to homeland security that the country faces today are challenging issues for leaders in Congress and the administration. In the Department of Homeland Security, where it is the plan to spend large amounts of money reasonably quickly, we need a disciplined portfolio investment process which will guide the department toward a better overall outcome within its budget constraints. Such a process would require a common threat vulnerability assessment approach, a common measure of risk, a process to rank-order investments using cost-benefit analysis and resource allocation methodologies, and finally, a means to link these decisions to the budget and procurement process.

To advance this effort, we have developed a framework to help senior policy-makers think through these issues called the security portfolio investment approach. The approach borrows from analytical tools that corporations use to assess the attractiveness of investments in the private sector today.

Another approach could be developed; the point here is that one should be used to make these complex decisions. The framework is dynamic, it will require difficult judgments, but these challenges can be managed. Use of an approach like this one will help ensure that taxpayer dollars are used wisely to fight terrorism.

Once the Department establishes its investment priorities, it will need to turn to the private sector to carry out key projects that advance the policies developed by Congress and the administration. Procurement, therefore, is the second area I would like to discuss today.

It is imperative that U.S. citizens get a strong return on their investment in the private sector's effort to develop homeland security solutions. The entire Department of Homeland Security system of buyers for information technology, intelligence and management services have to reach agreement on needs and desired outcomes, and these needs must then be translated into the requirements that drive the procurement process.

Five important steps directly related to the procurement process should be followed to accomplish better results for the Department of Homeland Security. In this case, better results mean successfully engaging the private sector to provide end-to-end solutions for homeland security that work, providing sound value to the government buyer and minimizing the risk to Congress and the taxpayer that public funds are poorly spent. All five steps are discussed in my written testimony, but the most important one is that we must ultimately have basic requirements, frameworks, standards and architectures for homeland security systems that we purchase.

To be certain, the administration has asked industry to develop these basic requirements and standards already, but in the current economic climate the lack of a process to develop an industry solution and competitive disincentives have kept many industries from taking the necessary steps to ensure an adequate level of increased security investment. Industry measures have been insufficient in the area of cybersecurity and in the chemical and trucking industries. Almost 2 years after 9/11 there are few agreed-upon standards for homeland security.

The extent to which government should be involved in the process of standard setting is open to debate. I believe there is a range of possible roles from government inspiration all of the way to government regulation that makes sense, but it is vital that government ensure that standards are ultimately set. The private sector will require varying degrees of help in this respect, but we must have agreement on standards to diminish waste between incompatible solutions and efficiently move solutions to scale.

In conclusion, the Department of Homeland Security should adapt private sector portfolio investment tools to inform decisions about how to protect our Nation against the threat of terrorism. This will help Congress resolve the difficult debate about how much and where to spend money on homeland security. Furthermore, the Federal Government can more effectively harness the capabilities of the private sector in the procurement process by ensuring that reasonable standards are developed. This will help optimize our investments, improve security, and deliver value to the American taxpayer.

Mr. CAMP. Thank you.

[The statement of Mr. Gould follows:]

PREPARED STATEMENT OF W. SCOTT GOULD

I. Introduction

Thank you for inviting me here today to participate in this discussion of *Best Business Practices for Securing America's Borders.* The previous witnesses have focused their remarks on the specific kinds of systems and technologies that we need to utilize to secure our land borders and other ports-of-entry, and prevent the entry of terrorists and weapons of mass destruction to our shores. I will focus my remarks in a different but equally important direction, specifically on the "best practices" that the government can utilize to ensure that it makes appropriate and beneficial investments in homeland security over the long-term. In particular, I want to discuss best practices in two key areas—portfolio investment and procurement—with a specific focus on homeland security.

This is a subject that my company, The O'Gara Company, has been focused on for the past 18 months in its efforts to help the private sector understand homeland security and the private sector's role in this critical endeavor. In May 2003, we published a report that summarized our accumulated knowledge on this topic, entitled "The Homeland Security Market: Corporate and Investment Strategies for the Domestic War against Terrorism," which was co-authored by one of my key staffers, Christian Beckner. That report was an attempt to provide corporations and investors with the essential facts that they need to know in order to do business in the homeland security market. Key excerpts from this report can be found at the end of my written testimony, and I would be happy to make full copies of the report available to members and their staffs at their request after the hearing.

The Department of Homeland Security has made rapid strides since its inception earlier this year, moving from what Secretary Ridge described as the "visionary phase" to the "implementation phase." Progress is being made every day, but we cannot underestimate the difficulty of this undertaking. We could cite numerous examples from the private sector of failed mergers and difficult restructurings. The Department is bringing together 22 diverse agencies, and at the same time building a number of new capabilities that will improve this country's ability to prevent and respond to terrorism.

Any successful business needs to understand and continuously improve its core business processes, such as its customer management, human resources, and financial accounting processes. Two key processes in any company are corporate budgeting and supplier management. The comparable functions in the federal government (and specifically in the Department of Homeland Security) are portfolio investment and procurement. I would like to examine each briefly, and discuss best practices for each. It is imperative that the Department and its constituent agencies study examples from the public and private sector and move vigorously to implement best practices in these two areas. If it can adopt effective capabilities in each area, the Department will improve its ability to make appropriate and cost-effective investments in homeland security.

II. Best Practices in Homeland Security: Portfolio Investment

Making appropriate investment decisions and allocating resources in alignment with the threats that we face is perhaps the most vexing issue for the homeland security leadership in the Administration today. How do we know where the threat is coming from? What targets should we be protecting, and from what kind of attacks? Should we focus our limited resources on preventing and detecting attacks or responding to the consequences of attacks? Which means should we use to prevent particular types of attacks? How many layers of security do we need to protect against any particular scenario?

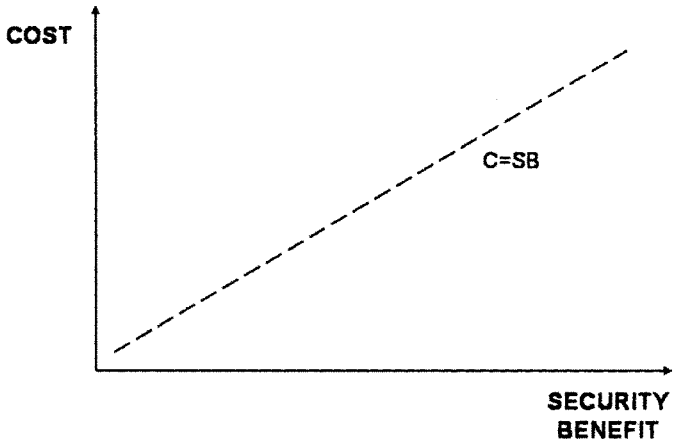
The efforts to improve our homeland security are not served by a collection of isolated investment decisions, each made without a common plan by competing bureaucratic interests. Homeland security is strengthened most effectively when our limited resources are managed in a coordinated fashion. The private sector regularly uses portfolio investment techniques to manage financial, technical and human resource allocation decisions. I believe we should do so in homeland security as well. Importantly, the public sector is familiar with these tools and they are already public law. For example, the Clinger-Cohen Act requires this basic management strategy to be used to guide information technology investments, and the GPRA planning and measurement process has acquainted government managers with planning and performance measurement techniques. In the Department of Homeland Security, where a large amount of money is being spent quickly, we need a disciplined portfolio investment process which will guide the Department toward a better overall outcome within its budget constraints. Such a process will require:

- A common threat vulnerability assessment approach
- A common measure of risk
- A process to rank order investments using cost-benefit analysis and resource allocation methodologies
- A means to link these decisions to the budget and procurement process

To advance this effort, we have developed a framework to help senior policy-makers think through these issues: the Security Portfolio Investment Approach (SPIA). The matrix borrows from analytical tools that corporations use to assess the attractiveness of investments. Any corporation has a range of competing options for future investment, which offer different rates of return. Similarly, the Department of Homeland Security has a range of projects that it could undertake to improve our homeland security. Some of them are low-cost quick fixes, and others are high-cost endeavors. Some of them offer only marginal improvements to our security; others could make substantial contributions to our security and plug a critical gap in our nation's defenses. The SPIA matrix allows the Department to weigh these trade-offs between cost and security, conduct an informed dialogue with the private sector, and choose the right projects for investment.

Chart 1 below shows the Security Portfolio Investment Approach and its two key axes:

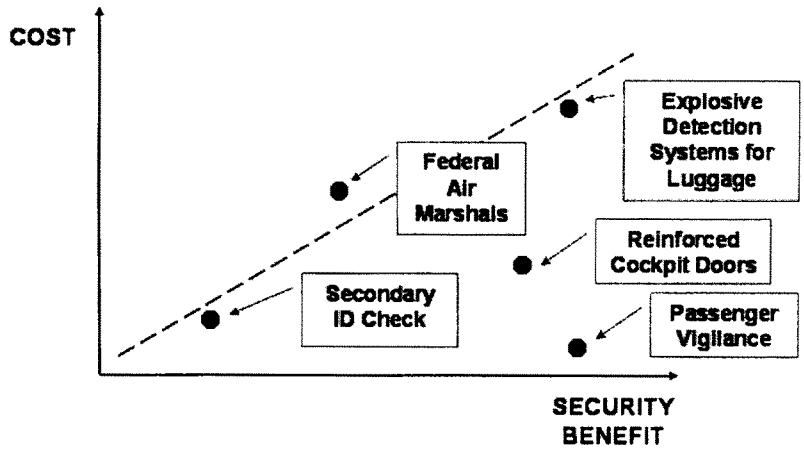
Chart 1: Security Portfolio Investment Approach (SPIA)



Any particular project can be placed on the chart according to its expected cost and its benefit from the standpoint of security. The dotted line that runs through the middle of the chart is a cut-off point between necessary and unnecessary projects. The benefits of projects that fall below the line outweigh their costs, and our desirable. Conversely, projects that fall above the line are expensive relative to their expected benefits, and should be funded only with great caution.

Chart 2 below shows the SPIA matrix in action, with examples from the area of aviation security, where the federal government has taken a number of important steps since 9/11 to improve security.

Chart 2: SPIA with Aviation Security examples



In the chart, we've plotted a number of key aviation security projects on the matrix. The placement of each project here is subjective, and based on public perception of the efficacy of these efforts, not any insight based on classified information about the TSA's performance. Some projects fall well below the line, such as the reinforcement of cockpit doors in commercial aircraft: this was a one-time, relatively low-cost expense that created a new and critical barrier to a repeat of the attacks of 9/11. Other projects that fall closer to the line are more difficult to judge. It is inexpensive to check traveler IDs for a second time at the departure gate, but the benefits of this are small in our assessment. It's a close call. The financial investment in Explosive Detection Systems (EDS) for checked baggage is significant, but the benefit of plugging this gap is correspondingly large, and worthwhile. Other projects fall above the line and are questionable. The increase in investment in federal air marshals is questionable in our opinion, given the fact that the reinforcement of cockpit doors and the likelihood of increased passenger vigilance (what we saw with the heroes of Flight 93, and the passengers who stopped Richard Reid from carrying out the shoe-bomb attack last year) already have created significant new layers of security in the cockpit and passenger cabin. Again, let me reinforce that this is based on a subjective interpretation of publicly available information; perhaps there is classified information that the increases to the federal air marshal program are in fact effective, but I have not seen this.

The main point of bringing up these examples is to illustrate how the SPIA matrix works, not to invite a prolonged discussion of these specific examples. This model could equally be applied to the topics of today's hearing, border security and trade security. In the area of trade security, you could plot projects such as the Container Security Initiative (CSI), the Customs Trade Partnership against Terrorism (C–TPAT), the 24-Hour rule, and R&D for next-generation cargo tracking and screening technology on the matrix. For border security, you could plot projects such as US VISIT, the National Security Entry-Exit System (NSEERS), investments in new motion sensors on the northern and southern borders, and changes to the Visa Waiver Program on the matrix.

It should be borne in mind that this framework is not intended to paint a static picture. A project could move to a new position on the matrix, and become more attractive, if one of the following happens:

1. A particular type of threat becomes more important. For example, after the near-miss of an Israeli jet-liner by a surface-to-air missile in Mombasa, Kenya last November, the danger posed by this type of threat from al-Qaeda became more significant, and investments in anti-missile technology (systems that use flares and chaff to misdirect incoming missiles) became more viable, shifting to the left on the matrix.

2. A project can be delivered at a lower cost. A technological breakthrough or increased vendor efficiency and competition could decrease the cost of a particular project. The project would shift downward on the matrix and become more viable.

3. Two projects are complementary in nature and create new value in combination. For example, two distinct database projects to track terrorists might be

marginal investments on their own, but in combination, create new information that significantly improves law enforcement officials' capabilities to stop terrorists in their tracks.

4. A project creates secondary value and improves business efficiency. Some of the programs that Customs and Border Protection (CBP) have undertaken in the past two years fit this description. The technology investments that companies will make to fulfill the requirements of the 24-Hour Rule and C–TPAT could also be used to improve supply chain efficiency, and facilitate the expedited sorting and delivery of inbound goods. These efficiencies can decrease the cost burdens to the private sector from new homeland security requirements.

Conversely, a project could become less attractive if another project makes it redundant. In the absence of reinforced cockpit doors and increased passenger vigilance, an increase in federal air marshals would be a wise investment. But in tandem with these other low-cost investments, it seems to deliver a low level of marginal security benefit at a high cost.

There are three key obstacles to the effective utilization of the SPIA matrix or a similar resource allocation model in the area of homeland security:

1. Difficult to know which threat scenarios to protect against. The US government has developed a large body of intelligence about al-Qaeda and other key terrorist organizations, and has some insight into their capabilities, interests, and preferred modes of attack. Nevertheless, it is difficult to set priorities among different threat scenarios. And it is even more difficult to get information about these priorities to the people who make the decisions about where to focus investment in homeland security, not only in the key agencies of the Department of Homeland Security, but also in the private sector, which owns more than 80 percent of the nation's critical infrastructure. New systems and processes need to be created to share this information with key decision-makers, without losing control over the information and tipping off terrorists about the focus of our efforts. A new system should be put in place to provide private-sector Chief Security Officers with clearances that give them access to critical information for their industries.

2. Difficult to quantify the effectiveness of any particular measure. There has not been a successful attack by al-Qaeda on US soil since the terrible day of September 11, 2001. Do we know why this is, with any certainty? Is it due to our offensive counter-terrorism efforts, in Afghanistan and dozens of other countries around the world? Is it due to the new capabilities given to US law enforcement agencies in the Patriot Act? Is it due to our investments in homeland security in the past twenty-two months, first in aviation security, and more recently for bioterrorism, border security, critical infrastructure protection, and port and cargo security? The federal government needs to develop classified capabilities to measure effectiveness, and understand what is deterring and preventing new acts of terrorism.

3. Difficult to measure the indirect costs of any security investment. It is easy to calculate the direct costs of a given security measure, as a line item in an agency's budget justification or an expenditure within a corporation's security budget. But it is not simple to account for key indirect costs. What is the overall cost to the American economy if trucks face significant delays at the Canadian and Mexican borders, or if cargo containers stack up at ports-of-entry due to new screening requirements? What is the societal cost of a project that has a significant negative impact on the civil liberties and privacy protections of US citizens? These are often subjective calculations; it is possible to come up with widely different estimates, depending upon what assumptions you use about the economic value of these items.

These three obstacles create challenges to the development of a portfolio investment framework and resource allocation process for the Department, but these challenges are not unsolvable. It is critical that the Department move forward to develop capabilities to make these assessments, and ensure that taxpayer's dollars are used wisely to fight terrorism. I hope that you and your fellow Members of Congress, as stewards of these resources, will provide the Department with the tools that they need to adapt best practices from the private sector and make effective investments in homeland security.

III. Best Practices in Homeland Security: Procurement

Once the Department establishes its investment priorities, it will need to turn to the private sector to carry out key projects that advance the policies developed by Congress and the Administration. Procurement is another area where attention to best practices is essential; in the area of homeland security, it is imperative that US citizens get a strong return on their investment in the private sector's contribution toward the development of homeland security solutions. With the announced appointment of Greg Rothwell as the Chief Procurement official for DHS, I have the

utmost confidence that the procurement shop he runs will follow a full and open communication policy with industry, favoring early and arms-length interaction. Al Martinez-Fonts is also playing an important role, opening doors for the private sector to work with the Department.

But their actions alone will not be enough. The entire DHS system of buyers for information technology, intelligence and management services has to reach agreement on needs and desired outcomes and these needs must be translated into the requirements that drive the procurement process, before even the most talented management team can deliver results. The term "results" in this case means: successfully engaging the private sector to provide end-to-end solutions for homeland security, sound value to the government buyer, and minimum risk to Congress and the taxpayer that public funds are well spent. Five important steps directly related to the procurement process should be followed to accomplish these results:

1. Build the capability to develop basic requirements, frameworks, standards, and architectures for HLS within the DHS

The administration has asked industry to develop basic requirements and standards. But in the current economic climate, the lack of a process to develop an industry solution and competitive incentives has kept many industries from taking the necessary steps to ensure an adequate level of increased security. Industry measures have been insufficient in the area of cyber-security, and in the chemical and trucking industries. Almost two years after 9/11, there are few agreed-upon standards for homeland security.

The Department needs to develop a capability to set standards as a cross-check for industry solutions, and as a credible alternative when an industry fails to step up to the plate. This capability must be established more quickly than current hiring activity at DHS indicates, and using private and non-profit technical expertise. Some of the reporting requirements related to standards in the FY 2004 appropriations bills will help DHS officials to focus on these issues.

2. Work with the private sector to create rapidly scaleable homeland security solutions, by using pilot projects to demonstrate existing industry solutions and build new systems from proven components.

Such programs should employ commercial off-the-shelf technologies in new ways to address emerging HLS market requirements and to reduce execution risk of near-term operational systems. Pilot projects need to be designed, funded, and managed to completion more quickly than is currently the case, and the use of commercial off-the-shelf technologies will help to speed up the process. Standards should be a key component of these pilot initiatives.

For longer-term projects, the new HSARPA should adopt proven DoD 5000 methodologies for research, development, and prototyping, and bring DoD expertise to bear on development of these new technologies.

3. Where industry is taking the lead to develop standards, the DHS needs to push for accountability.

The Department needs to create deadlines for industry proposals to create their own standards, and push them toward intra-industry cooperation. It needs to provide a forum for discussion of these issues, and draw public attention to the need for standards and a generally agreed upon solution.

4. In the absence of consensus on standards by the deadline, DHS and other federal agencies (e.g., Department of Transportation) should take control and move the process into a rule making or regulatory framework.

Here the federal government can make some of the key technical calls that hinder agreement, choose the best system and set standards.

The choices between basic requirements, frameworks, standards and architectures can be tantamount to a choice between different technology solutions and products. But such choices also remove investment risk for the private sector, and will stimulate their investment in compliant technologies, improving the industry's security.

The value of the many pilot projects that are currently underway within DHS can only be harvested when the government takes the results of the pilots, makes a decision about overall architecture, and applies these lessons to choose the best solution.

5. Increase transparency of information about procurement opportunities.

The government website Fedbizopps.gov states that it is intended to be the "single government point-of-entry for Federal government procurement opportunities over $25,000." But the site is used unevenly by government procurement organizations. Small-scale procurement opportunities, for janitorial services and uniforms, are often found on the site, but information about larger, more strategic projects is

sometimes missing. And the site provides no means for companies to learn about opportunities that are sourced using Government Wide Acquisition Contracts (GWACs) or opportunities as subcontractors on large projects. Greater transparency would increase the involvement of small firms in the procurement process and lead to more robust competition.

The extent to which government should be involved in the process of standard setting is of course open to debate. I believe that there is a range of possible roles—from government inspiration to government regulation. But it is vital that government ensure that standards are ultimately set. The private sector will require varying degrees of help in this respect. But we must have agreement on standards to diminish waste between incompatible solutions and efficiently move solutions to scale as we work to improve public safety and security here at home.

IV. Conclusion

The Department of Homeland Security should develop best practices in the two key areas discussed above. It should adapt private-sector portfolio investment tools to inform decisions about how to protect our nation against the threat of terrorism. If we don't address the right threats and focus in the right areas, there could be critical gaps in our ability to deter terrorism. Portfolio investment tools are ideal for this purpose and should be employed by Agencies, OMB and Appropriators. Furthermore, the federal government can more effectively harness the capabilities of the private sector by ensuring that reasonable requirements, frameworks, standards, and architectures are developed to optimize our investments, improve security and deliver value to the American taxpayer.

V. Key Excerpts from "The Homeland Security Market: Corporate and Investment Strategies for the Domestic War against Terrorism."

On public-private cooperation:

"Right now, the United States finds itself at a pivotal point in the evolution of homeland security. The success or failure of the government's efforts to improve the country's defenses against terrorism depends upon a number of factors, not least of which is the effectiveness of its interactions with the private sector. The private sector has often lacked a sophisticated understanding of government behavior, and the government's outreach to the private sector has been haphazard. A new spirit of public-private cooperation is essential for the successful implementation of a national homeland security strategy."

On integrating an understanding of the terrorist threat into companies' strategies:

"Smart companies can increase their chances of developing partnerships with the federal government if they develop systems and solutions that protect the country against threats that are real but not yet high on the government's radar."

On the size of the homeland security market:

"Many analyses of the homeland security market have confused the federal government's budget for homeland security with the size of the homeland security market. . . . The size of the US federal homeland security market is estimated to be the following: $7.26 billion in FY 2002, $6.13 billion in FY 2003, and $7.21 billion in FY 2004."

On the role of integrators in carrying out homeland security projects:

"The Integration category includes companies that are responsible for piecing together disparate technologies and processes to create functional homeland security systems. Firms in this category can be classified into four industry groups: aerospace, consulting, IT and high-tech, and specialized government contractors. . . These firms play a key role in homeland security because of the market's heterogeneity and complexity. Only they have the capacity to develop cross-cutting solutions and solve problems for the government. The homeland security market is made up of businesses in a range of industries—including information technology, telecommunications, aerospace, management consulting, logistics, engineering, high-tech equipment, biotechnology, and human resource services. This long list is far from exhaustive. However, among the industries participating in the homeland security market, only a handful have the capability to provide the government with fully-elaborated "solutions" to many of the homeland security challenges that it faces. For example, upcoming efforts to create a new border security entry-exit system will require input from companies focused on biometrics, physical security, database integration, vehicle scanning and identification, and secure communications, among others. Only companies like the ones above could manage such a project and mold these disparate technologies into an integrated system."

On the security value of homeland security investments:

"A good homeland security investment should offer clear and compelling value to a government buyer, who responds to different incentives than a typical private-sector buyer, as discussed in Section 1.1. The product or technology should deliver a comprehensive "solution" to the government, and the company should be able to describe this solution in an elevator speech. If a company can say convincingly that Product X provides an end-to-end solution to protect the country against the container security threat, for example, then it will have an advantage over competitors that offer only stand-alone technologies or parts of solutions. And if a company can say, without exaggeration, that with a certain product or technology "the 9/11 terrorists would have never made it on the plane that day," then the company is being responsive to government buyer values."

On the effect of privacy on homeland security investments:

"The right to privacy is a fundamental and fiercely protected value in the United States and other parts of world, and numerous advocacy groups relentlessly highlight any adverse impacts on privacy rights. Many homeland security initiatives have been stopped in their tracks during the last 20 months due to privacy issues, such as Operation TIPS, an effort to enlist several million citizen informants; and the boldly named Total Information Awareness program, designed to troll private sector databases in search of patterns of terrorist behavior. Any potential product or technology needs to be conceived with this constraint in mind; and breakthrough technologies that increase security without having a negative impact on privacy could be particularly attractive."

On the effect of business efficiency on homeland security investments:

"Another constraining force on homeland security products and technologies is their impact on business efficiency, both from a business unit-level operational perspective and from a system-level supply chain perspective. From an operations standpoint, if a baggage screening system at an airport provides 100% detection of explosives but can only scan one bag per minute, then it will cause unacceptable bottlenecks at airport check-in points. The right balance needs to be struck in any system between security and operational efficiency: this balance will depend on an assessment of the threat and the severity of the economic impact of the security measures. This same dynamic holds true for the global supply chain. For example, if a cargo container inspection system improves security but severely disrupts the normal flow of commerce between and across national borders, then its application becomes infeasible. Products and technologies that both improve security and business efficiency are likely to be particularly attractive targets for investment. Such products have dual-use futures; for example, a system to improve the security of commercial trucks could also have applications that improve fleet productivity."

Excerpted from "The Homeland Security Market: Corporate and Investment Strategies for the Domestic War against Terrorism," by W. Scott Gould and Christian Beckner, The O'Gara Company. May 2003. Copy can be ordered for no charge at http://www.ogara.com/.

Mr. CAMP. Mr. Katz.

STATEMENT OF B. JEFFREY KATZ, VICE PRESIDENT OF MARKETING, ATMEL CORPORATION

Mr. KATZ. Thank you, Mr. Chairman. Atmel Corporation appreciates the opportunity to testify before the subcommittee.

Atmel is a semiconductor manufacturer. We make computer chips, and our chips are used in systems. We are also a principal member of an industry and government consortium called The Smart Card Alliance, which is a group of competitors and interdependent companies that promote and educate the public on the use of security technologies both for personal identification as well as transaction activities such as bank cards. I am going to talk about something a little different from those things today, but I wanted to give you that background.

Today I am going to testify about some technologies that can be used for container security.

Since September 11, much of the attention that the public has had on homeland security has been aimed at personal access into

the country. This is similar to, but different from the port security where I am going to talk about container security.

Cargo containers, unlike people, cannot be identified by biometrics. They are, by their very nature, anonymous. They look alike and they spend considerable amount of time where they may or may not be monitored.

There is a guy, Mr. Stephen Flynn, who is a national security expert at the Council on Foreign Relations, and he observed, "The bottom line is that anybody in the world right now who has between $1,600 and $3,000 and 30 tons of material can order a box, have it delivered to their home or workplace. They can load it to the gills, close the doors, put a 50-cent lead seal on it, and it is off to the races."

Today, there is some 12 million cargo containers in the world, and every year about half of them go through U.S. ports. They travel on the back of trucks all over our country, and they contain the same tamper-evident technology to secure them that was in use at the time of Alexander the Great. We can do better.

We believe the DHS must and is playing a leadership role in improving container security in our ports and around the country. In particular, much of this testimony relates to secure container initiatives. There are two major requirements, and I am not going to be an expert on both of them.

The first is that the system integrator contractors, as well as the shipping companies, must be encouraged to adopt and support the available technology. I will help you on that if I can. But the second one is that the Department and the government must establish and negotiate appropriate policies and procedures to be followed worldwide by our trading partner countries and shipping companies at the point of origin and all throughout the transport life of a container.

With the technology I am going to show you and reliable inspections at the source, a precise history of container movement and activity getting in and out of the opening of the container, as well as its contents, can be logged for use by receiving inspectors and logged in the container itself. Using relatively inexpensive, embedded security chips, global positioning chips and license-free radio receiver chips, as well as Smart Card worker IDs, every access to the container, by whom, and at which precise location can be safely stored in tamper-resistant devices that are built into and control the container locking mechanism.

Mr. KATZ. And container activity history can be broadcast wirelessly to logistic centers and inspection points. Even as the cargo liner approaches the port, the Coast Guard or Customs officers can receive encrypted information directly from each container indicating what is in it and what containers have been opened, by whom and where since the original embarkation inspection, and which containers have remained intact.

We hope the committee will encourage the DHS to accelerate programs to enhance container security with this easily available technology. The technology is only part of the solution. It is for the Department and our diplomats to negotiate the policies to use the technology. I hope to show you that the technology exists today.

Please refer on your desk, you should have a little handout here. I would like to walk you through a couple pages of it.

The first page is called system architecture, and there you see a cartoon that implies a cargo liner on the left with its own GPS navigation equipment, as well as containers. Each container has a secure locking unit, which also has an ISM band license-free wireless transmitter and a GPS receiver. Each GPS receiver is only about a square inch, a little module about a 16th of an inch thick.

With those electronic items on the container, each container can communicate with the ship when it is in port—or when it is underway, and unavailable to the GPS system, any accesses to it. When it is in port or on a truck and the container is exposed to the sky, then it knows exactly where it is and can broadcast that to control centers.

If you flip down to the third or fourth page down, the one that says "container access control," you can see that there can be attached to each container a small module which manages the lock on that device, much better than a lead seal. It has in it an embedded security chip, which can hold encrypted and tamper-resistent information, and it also has within it the transceiver chip which allows the container to broadcast activity to a local control center, or using the GSM system worldwide, even through the phone lines could send long distance remote messages.

To access the container, an authorized user will have an ID card which wirelessly can unlock it while the lock module logs who it is that is doing it. This can also be done with biometrics to indicate the authenticity of the user.

So that is the heart of the system, and then it takes, of course, the back-room stuff that goes into the control centers to manage it.

So the last page of the handout indicates some of the chips which are all available today. These are available from my company Atmel, but also from companies as well. The GPS receiver module, I mentioned earlier, is about a square inch. There is also the tamper resistent smart card microcontroller chip that is used in bank cards and in telephone communication cards, as well as personal ID systems; and the license-free ISM transceiver chips, those are individual single chips. Nothing on that chart costs more than about $10, and so even if you put them inside the bombproof, bullet-proof boxes, it is an economically attractive, commercially available system. We hope the committee will encourage the Department to use such technologies.

[The statement of B. Jeffrey Katz follows:]

PREPARED STATEMENT OF B. JEFFREY KATZ

Atmel Corporation appreciates being invited to testify before this committee. I'll briefly describe Atmel and myself as a witness.' Based in San Jose California, Atmel is a publicly owned 18-year old semiconductor manufacturer. We make a broad range of integrated circuits in our plants in Colorado and in Europe, including several types that are directly aimed at security applications such as Smart Cards for banking, personal identity, computer security, and telecommunications, biometric scanners, and a variety of radio frequency communication chips. Atmel's annual revenues comprise about $1.2 B, more than half of which is shipped outside the US, making us a net exporter. I was educated as a computer engineer. I have worked for Atmel for about 14 years, in my current capacity. Before joining Atmel I held various design engineering, marketing and operational jobs at Unisys, Encore Computers and Intel Corporation.

Atmel is a principal member of an industry-government consortium called the Smart Card Alliance. Its members, comprising interdependent, sometimes competing enterprises, cooperate to educate potential users of Smart Cards and related security technologies, and advocate their use where appropriate. The Alliance is active in publishing white papers and presenting seminars, especially in the areas of secure personal identification, physical access, biometrics, and transaction processing. Some if these educational activities have been aimed at Department of Homeland Security programs such as the Transportation Workers 10 Card, and the US Visitor program. I have been personally involved in many of these activities as a contributing author and seminar presenter.

Atmel, and the Smart Card Alliance would like to commend DHS leadership for taking initiatives to be visible and forthcoming in explaining their needs and their opportunities for industry engagement, and receptive to inputs. It's not always as easy as we would like for industry participants, especially subcontractors to the primes, to locate decision-makers in the Department. But we believe the Department is moving in the right direction and exercising its leadership role.

Since Sept. 11, 2001 the American public, the Congress and the newly formed DHS have paid considerable attention to the issue of personal identification. The notion of assuring that individual people are indeed who they say they are, and that they are authorized to access certain physical premises and electronic networks, has been thoroughly scrutinized and several programs are in pilot phase to evaluate technologies and operating procedures. Indeed my own company has been active in proposing some of these identification systems. This testimony is aimed at a different aspect of Homeland Security, protecting our ports of entry in the area of cargo container security. This aspect represents a potentially far greater vulnerability than that of individual people gaining inappropriate access. Especially in light of the highly conspicuous personal security screening that we have deployed in the past two years, and the increased interest in using biometrics and other sophisticated means to authenticate personal identity.

Cargo containers, on the other hand, are by their very nature fairly anonymous They look pretty much alike, they spend considerable time exposed in relatively non-secure environments, often unattended and unmonitored, and they can hold significant amounts of potentially dangerous material. .

Mr. Stephen Flynn, a senior national security expert at the Council on Foreign Relations, has observed: "The bottom line is that anybody in the world right now who has about $1,600 to $3,000 and 30 tons of material can order a box, have it delivered to their home or to their workplace. They can load it to the gills, close the doors, put a 50-cent lead seal on it, and it's off to the races."

Today there are some 12 million cargo containers in use worldwide. Every year roughly half of them come through US ports. And they travel on the back of trucks all over our country. With the same tamper-evident security technology that was used in the time of Alexander the Great.

At Atmel Corporation, we believe the issue of container security has been relatively less explored, both by the DHS and by the media. And we believe there are readily available technologies that can be deployed fairly inexpensively, to considerably improve this potential weakness in our national security. Today I plan to describe to you some off-the-shelf semiconductors that can significantly upgrade container security. This semiconductor technology is all available from Atmel Corporation, as well as several other chip makers.

We believe DHS must and is playing a leadership role in improving container security in our ports and around the country. In particular, much of this testimony relates to the Secure Container Initiative. We believe there are two major requirements: System integrator contractors, as well as shipping companies, . must be encouraged to adopt and support the available technology. And the Department must establish appropriate policies and procedures to be followed worldwide by trading partner countries and shipping companies at the origin point of cargo shipments, and along all the stages of transport to out port of entry and beyond. With this technology, and reliable inspections at the source, the precise history of container movement, as well as contents, can be logged for use by receiving inspectors. Using relatively inexpensive embedded security chips, GPS chips, license-free radio transceiver chips, and wireless Smart Card worker and inspector IDs, every access to each container, by whom and at which precise location, can be safely stored in tamper resistant, devices that are built into and control the container locking mechanism. And container activity history can be broadcast wirelessly to logistics centers, and inspection points. Even as the cargo liner approaches a US port, Coast Guard or Customs officers can receive encrypted information directly from each container, indicating what is in each container, which containers have been opened, by whom and where, since the original embarkation inspection, and which containers have re-

mained intact. We hope the Committee will encourage DHS to accelerate programs to enhance container security with this easily available technology. The technology is only part of the solution. It's for the Department, and our diplomats, to negotiate policies to use the technology. But I hope to show you that the technology exists today.

Please refer to the attached diagrams for a brief explanation of how these technologies can be deployed to greatly improve container security.

Thank you again for the opportunity to testify before the committee. Atmel is always available to discuss these ideas, as well as our technologies and proposals for secure personal ID, with appropriate people in the Committee, the Department, and the system integrator contractor community.

U.S. House of Representatives
Select Committee on Homeland Security

Testimony of

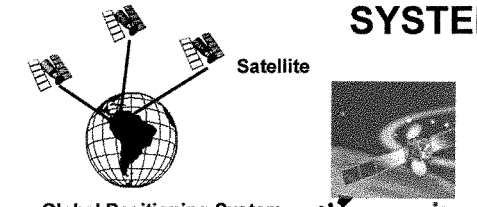
B. Jeffrey Katz

Vice President of Marketing
Atmel Corporation
San Jose, California

July 23, 2003

Technology for Port Security: Using readily available, commercially economical semiconductors, secure and track access activity of cargo shipping containers. Record all container accesses in tamper-resistant modules, and make log information available to TSA authorities wirelessly.

SYSTEM ARCHITECTURE



Container

GPS Receiver on liner -Off-shore Positioning	GPS Receiver On container -On-shore Positioning	ISM Band Transceiver on each container - Logistic Management - Identification	Lock unit -Secure Logging

Cargo liner

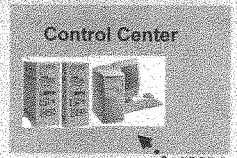
Off-shore cargo:

1. The GPS receiver for navigation on liners positions off-shore cargo.
2. Data sent to on-shore control center by satellite link
3. Control center checks and manages cargo before embarkation

On-shore

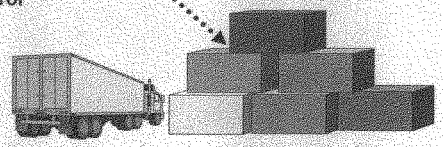
On-shore cargo:

1. ISM Radio link between containers and control center.
2. Logistic control from center
3. GPS receivers on containers position on-shore cargo beyond the reach of ISM radio link.



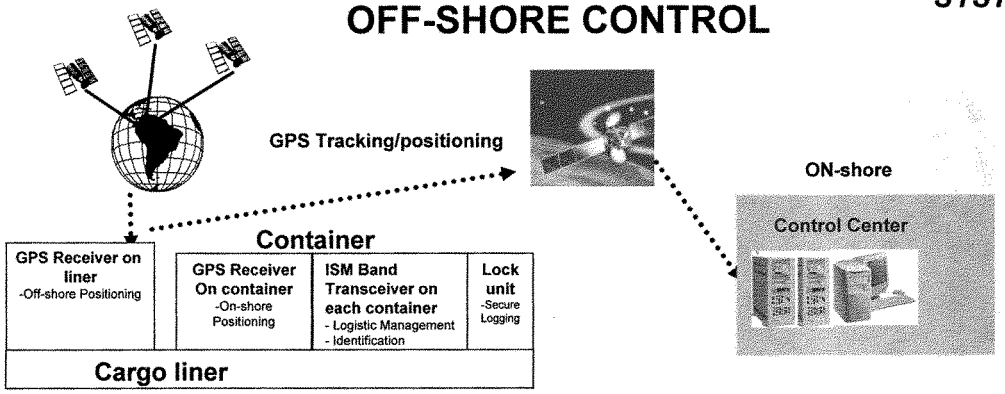
ISM band radio link

Logistic control



container

OFF-SHORE CONTROL



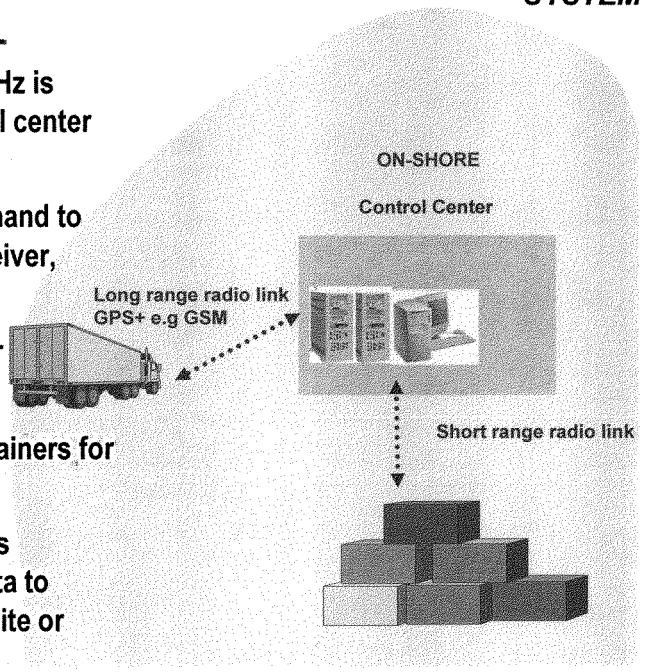
1. GPS receiver installed on liner positions and tracks the liner.

2. Position, velocity and time are transmitted, with cargo information to on-shore control center via satellite.

3. Control center controls and monitors sea traffic and cargo, and co-ordinates on-shore operation simultaneously for proper and secured embarkation.

ON-SHORE CONTROL

1. license free ISM band 915MHz is established between control center and container
2. Control Center sends command to activate AT86RF211 transceiver, working in pair.
3. Container sends ID code for identification.
4. Control Center locates containers for logistic purpose
5. GPS receivers on containers position cargo and send data to control centers, using satellite or GSM links.



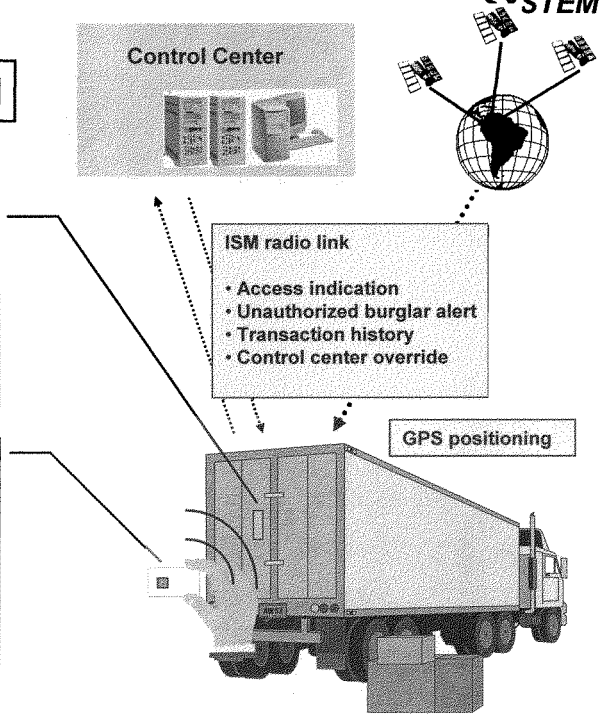
Container Access Control

Secure Access System Unit

- Door lock system control
- Access control
- Location-aware
- Personnel access log, time stamping, location stamping... etc

Contactless Secure Memory Card (CryptoRF)

- Personnel identity
- Authentication
- Access level
- Other secure information



Container Access System Concept

- Authorized personnel own a smart card embedded with CryptoRF
- System unit makes use of contactless communication to the CryptoRF card
- Optional Biometric/PIN can also be implemented
- Each access is authenticated and logged. Data are transmitted to control center whenever link is active
- Unauthorized access or burglar activity alert alarms the control center immediately to prevent theft
- Control center override is possible, if required

OFF-THE-SHELF TECHNOLOGY FOR CARGO TRACKING SYSTEM

- GPS receiver chip set (Atmel ATR0600) positions and tracks cargo. Position, velocity and time are sent to on-shore control center via satellite, and/or logged in secure lock module.

- Secure, tamper-resistant Smart Card Microcontroller or Crypto Memory logs lock activity and permits only authorized container access

- License-free ISM transceiver chip (Atmel AT86RF211) establishes short distance radio link of 1km with control center.

Mr. CAMP. Thank you very much. Dr. Gould, I have a question about this decision-making framework you have sort of laid out here, which I appreciate you doing. You, also in your written testimony, mention that Congress needs to provide additional tools to the new department to help them to adapt these best practices as you have described from the private sector for investment decisions in homeland security.

Can you offer just a little more elaboration on that and whether you see these additional needs that Congress needs to address?

Mr. GOULD. Certainly, Mr. Chairman. I think importantly appropriators in the 2004 budget process have begun to identify very specific requirements for reporting from the Department of Homeland Security back to the Appropriations Committees that begin to lay some of this foundation. The most simple and yet—and most profound thing I think Congress can do at this stage is simply ask for that information. The Department of Homeland Security will then need to find the right kind of people and partners with the private sector to articulate what those requirements, standards and architectures are, and then bring that back to senior decision-makers and Congress at a very fundamental level. It would be enormously helpful to have that simple request and perhaps some earmarking or funding that would make that possible.

Mr. CAMP. Thank you.

Captain Salloum, you mentioned the various security programs and their overlap and the effect on the private sector, and I guess I would like to little further comment from you on the effect of this overlap on commerce and what might be done to streamline the process, obviously, to make sure that cargo is tracked and is screened and is secure, but if you could just elaborate a little bit, I would appreciate it.

Mr. SALLOUM. Thank you, Mr. Chairman. With regard to the tracking devices, this definitely is an important issue with regard to the security, but I believe also there are other ideas out there and opinions—the same thing that I am saying today. It is good to know where the container is, but it is very important to know what is inside of the containers.

And with regard to the overlaps, Mr. Chairman, Homeland Security, when they start—when the United States Government decides to protect our borders and they place all these initiatives, they are very good initiatives. And as I said in my testimony, it is a good start. And they couldn't do other than what they did, because the logistics systems already is fragmented.

As an example, one shipment starting from Mexico ending in the United States could involve about 19 different companies and 11 proprietary systems. So what that did is they took the flow of the shipments and they concentrated on the different entities. They set an example for the ports where we are going to place security container initiatives. For the corporate shippers, we are going to do C–TPAT, Customs Trade Partnership Against Terrorism. But we believe it is as important to have initiatives for the corporate shippers. It is also important to consider the individual shippers, because they do represent somewhere around 30 percent of the cargo getting to our countries.

So it is important to have one system—it could be one system like the airline industry, the system today managing the airline passenger ticket industry. We need such a system in the freight industry by which you can apply all this security measures, getting the data, global data and apply the artificial intelligence to protect our borders.

Protecting our borders, Mr. Chairman, doesn't start here. It starts from where the shipment originated, and also starts by knowing that particular warehouse, what his activity is, and this can be done only if we achieve what the airline industry has achieved from the passenger side, a horizontal system that provide about—I mean, provides efficiency, commercial benefit to the global logistics industry which they need it, definitely they need, and they will adopt it because they have commercial benefits to it. And then we can definitely have the security that we are seeking for. Thank you, Mr. Chairman.

Mr. CAMP. Thank you.

The Chair will now recognize members for questioning. The 5-minute rule will apply, and the Chair recognizes the ranking member, Ms. Sanchez.

Ms. SANCHEZ. Thank you, Mr. Chairman. I have various questions. First I would like to ask all of you, because it has to do with this whole issue of comprehensive risk and a vulnerability assessment of infrastructure, and we have been trying to figure out the Department of Homeland Security and how it is coming along with that particular assignment, let's say because we believe it is incredibly important, in particular if we are going to invest from a taxpayers' perspective in hardening some of this or in working with some of the cyber security issues that we have.

I would like to ask each of you as private companies, have you been working with the Department? Have they approached you? How have you found the process, if you have, or have they not even contacted you with respect to how to handle infrastructure assessment? I guess I would start with the Boeing company.

Mr. STEPHENS. Infrastructure protection—and I think the analysis you talk about, our observation is there are a number of elements within the Department making assessments in their particular areas, and I think the Department has yet to come together in a fully integrated way, you know, to look at that as an integrated system, not unlike a number of companies that come together—and I can use the Boeing Company example. As we have come together, it is taken a while to make sure we have got all our elements working together. There is a dialogue underway. I know that we are sharing information about the Boeing critical infrastructure that we have back with the different and the potential threats that go against our systems each and every day as we operate as a commercial enterprise, but I think the long and the short of it is there is a ways to go yet to get some consistency in the discussion standards between the private industry and the Department.

Ms. SANCHEZ. Very nice way of putting it.

Captain.

Mr. SALLOUM. Simple. No, we did not and they did not. And we believe—we know that after September 11, somewhere about

30,000 ideas have been presented to the United States Customs. So which one is the right one? So definitely it is an enormous task for them to decide which one is the right one. We can distinguish the system we are proposing from everybody else, because we have been working on it since 1998, and from a commercial perspective. It is to provide this horizontal approach for the corporate shipper, for the ports of Los Angeles to resolve the congestions at the port of Los Angeles.

So everybody in the system must have a benefit to the port, the corporate shippers, carriers, everybody. So we started doing this since 1998.

Now, after September 11, efficiency must iclude tracking. It means visibility. It means knowing where the shipment is and who loaded it and when it was loaded. It means three dimensional security. When I contract you to load it, how long can it take to load the containers? What is your forecast, how long should it take to get the shipment there? In reality, what have you done? This is three-dimensional security that not a lot of people talk about, which is important for the efficiency and commercial benefits.

So having said that, it is an enormous task for them to decide which technology is the right one, and we are working toward that to let them know that there are certain systems out there that could help their efforts to achieve the security we are seeking for.

Ms. SANCHEZ. Thank you.

Dr. Gould, since I used to work for Booz Allen, I love your little presentation and your thought processes. Can you tell us have you been consulting at all towards this measure with anybody in the Department of Homeland?

Mr. GOULD. Thank you for asking. One of the—the short answer to your question is obviously that comprehensive risk and vulnerability analysis has not been conducted. It has not been finalized, and it remains a barrier, I think, to the private sector being able to build the kinds of systems that we ultimately need. It is certainly a barrier to the private equity market that looks to pick technologies and pick winners early in the cycle without knowing which way a government will go, there is an enormous effect here in terms of market-making capabilities.

The O'Gara company has sponsored philanthropically a symposia with one of the leading think tanks here in town, the Center for Strategic International Studies. During some of those sessions we have had lengthy discussions of give and take at which members of the Department of Homeland Security were there. People like Al Martinez are doing a great job trying to open the doors and have communication. The new head of procurement, Greg Rothwell, for the Department of Homeland Security, is one of those open dialogue, open communication senior executives from the career branch, but in our view this is just beginning. It needs additional attention and focus.

Ms. SANCHEZ. Mr. Katz—and I would also like to have you answer—can you just sort of walk us through how much it would cost and whether these little chips are reprogrammable or whether you buy one each time for a container, and how do you know it is secure the whole way, I guess?

Mr. KATZ. I will answer the first question first, and then the more fun one, I suppose. In answer to your first question, Atmel has not been consulted by the Department of Homeland Security about infrastructure assessments. I doubt if they would have consulted with any semiconductor manufacturer in that regard. That is not what we do.

I can comment, though, that we have observed that the Department is very visible and forthcoming in describing what they think they need and also trying to give prime contractors access to them. It is not always apparent to a subcontractor like Atmel, where to go in the Department.

To your second question, all of the chips that I described earlier are indeed programmable. With appropriate authentication techniques their content can be changed. They can't be changed if you don't have the right authorization to do so. So each container can be used many times once you equip it.

Ms. SANCHEZ. And just—I know my time is up, but I have one little quick question on this issue. So we have got all these thousands—hundreds of thousands of containers, millions going around the world, and we have got these little chips on all of them. They are sending information. There are new satellites up there to have to move them and send it. Isn't that just a whole bunch of information going through the air, and where does it go? And how do we, on time, get to this so that we know someone has opened a container before it gets to Los Angeles, for example?

Mr. KATZ. Well, each container can take care of its own records. The satellite use is only to tell the container where it is so it can record that information. The satellites are there. They are being used all the time, and this is just another use for them. There is no special information about the container that goes through the satellites, unless some system were designed to make remote calls to report status. That isn't what we envision necessarily, though.

What is going to happen, though, is that in local control centers, whether they are at ports or on inspection ships or at cargo depots around the country, containers can broadcast locally, not all through the whole ether all over the world, but they can broadcast locally to inspection authorities which ones of them have been opened and by whom and when and where.

Mr. COX. Thank you. I want to again thank our panel.

I wonder if I can ask you to think beyond what we have been talking about here for just a moment to the question of incentives and how it is that we are going to get the private sector, which owns so much of our critical infrastructure and has so must have to do with achieving our objectives here to play along. One of the things that we have been talking about on this committee with other witnesses at other hearings is the liability system and the insurance system and whether or not these can be carrots and sticks that we use to bring people along. If we are trying to get people to deploy technologies, if we want to adopt the recommendations that you are making, how can we encourage people—how can we set up a system of incentives, restraints and penalties so that—in a Nation of 280 million people without a command and control system that we get the results we are after? Anyone that wants to leap at that with creative thought is welcome to do so.

Dr. Gould.

Mr. GOULD. Certainly. It is a terribly important question, because at the end of the day with over 85 percent of the critical infrastructure owned by the private sector and limited resources for the Federal Government, you have got to find some intelligent way to leverage resources.

I think one very important step has occurred with new SEC regulations requiring disclosures by large companies about the activities they are taking in the security arena. This is one imposes a cost on industry. It is minor, but it illuminates what companies are doing to secure users of their technologies and services. It seems to me a simple and effective thing, and perhaps additional attention in this area along disclosure and connection with the financial audits would have some substantial benefit.

The second area you already touched on had to do with the insurance industry. We have seen the benefits over time in property and casualty for fire insurance where the knowledge the insurance companies have, through a series of discounts on insurance premia, invite constructive actions that companies can take to reduce the risk of fire. Analogously, I think we could do that in the homeland security and terrorism arena by, again, developing standards, beginning to develop an industry perspective on what specific steps we need to do to harden targets, protect our cyber assets and the like and that those discounts over time would both create a market for that business and incentivize business to lower their costs and increase their investment in security.

Mr. COX. Mr. Katz, you also wanted to—.

Mr. KATZ. Yes. I would comment that in your earlier remarks, Mr. Cox, you mentioned that not only do we want to make sure the ports are safe, but that the material moves smoothly.

As Captain Salloum mentioned earlier, we need to do this globally. If we had a system where containers and shipping—the whole shipping system were known to be secure from the point of entry, from the point of origination until the point of entry and beyond—then we would make it pretty expensive if you are not part of that system to have to inspect individual containers that were not so protected, whereas allowing the protected and securely logged containers to flow through virtually uninspected. And the—.

Mr. COX. How would that expense be borne?

Mr. KATZ. By the shippers, I presume, the original people who consigned the materials. It would cost them more and take it longer to get the materials through—.

Mr. COX. The reason I ask is that obviously the ports are comprised of a lot of medium-sized enterprises, and I don't think what you want to do is set up a system that punishes them. They are not the shippers, and it is not within their control. So somehow you have got to put this cost on the shipper. How do you do that? With a tax, or what do you do?

Mr. KATZ. I guess that would have to go back to the shipping companies to be able to have a two-tiered rate. I am not sure we can legislate that or do anything more than encourage it, but we can say it is going to take longer if you do it the old way, and if you use the new technology, it gets through quicker, and there will

be that incentive for them to charge more to their originating business partners.

Mr. COX. Captain Salloum, you wanted to add also.

Mr. SALLOUM. Yes, sir. It is a very good question, and the system we are proposing or we are talking about is a system that provides—first of all, increases the ROI of every participant in the flow of a shipment, because we add to it efficiency. I can give you an example, because Ms. Sanchez used the port of Los Angeles as an example. One of the things for the port—I mean, when I say increase the ROI, we are talking about corporate shipper, low-volume shippers, carriers, ports, everybody involved in the supply chain. Also individual shippers, everyone involved in the flow of a shipment is a participant in the system, and they will increase their ROI and reduce their costs.

And to use that example, port of Los Angeles, port of Los Angeles by 2007, the statistics say they will be out of space and they cannot expand any more. And one of the things happening today from an efficiency side, containers are sent and triggered from the factories, all of them to the ports, and they stay at the ports waiting for the ship to come in. So this is an added cost to the shipper because he pay for the storage. Second, it is a problem for the port. He cannot expand no more. The key is in efficiency.

So what does that mean, efficiency? What we are talking about is the integration of the carrier service on the ship with the trigger of the cargo from the factory. So the cargo get triggered, integrated with the vessel, arrival to the port. So the cargo gets to the port, and we minimize the time of the container at the port so we will have the efficiency that port of Los Angeles requires. That is one.

Once we do that, what would happen? The shipper, he pays less storage. He is happy. The ship doesn't stop too much at the port because there will be a place to enter and move the—I mean, load or unload the containers. Port of Los Angeles is happy. Also from a security aspect, the container does not lay there for long time so there is less access for people to tamper into the shipment.

So as you can see, this is one example of 50 I can give you—provide you of how we can combine the commercial benefits and the security compliance; and in other words, the system must recognize—and we have these numbers we can provide you, sir, if you would like, those numbers. The system must recognize somewhere about 10 to 15 percent of saving on supply chain on individual shippers, and the system itself now will ask for 2 percent. It will fund itself. So we will ask 2 percent from these savings. And we will not charge any additional charges to anybody else involved in the shipment.

This is how it would work, and this is how you, sir, can guarantee the global participation so we know the activity of that famous warehouse in Yugoslavia, moving cargo from Yugoslavia to Italy. We will know what he usually moves, and to where, where he pick up his empty container and all of the above. So that is what the system needs in order to achieve security, local security. And by the way, sir, as you know, we do also have interests overseas, and it is important also to address that. Thank you, sir.

Mr. STEPHENS. Sir, Mr. Chairman, one of our observations as we are working in the aviation industry is it is a free market economy,

and free market economies tend to move based on the financial incentive rewards that all the participants participate in.

One of the things we noticed, and I am certain that you and your committee noticed is that when it came time for the implementation of the aviation security requirements this last year, you certainly probably got different feedback from the airlines that was different than the airports and was different than the other elements of the industry moving forward, plus the legislation that was put in place to go secure America's airports.

And it became very clear that the financial relationships were not well understood by all of the members. We have actually started an aviation security study that involves the Airline Transportation Association, the American executives for airports, the American Council—or the Airports Council International, the Transportation Security Administration. We have invited the Federal Aviation Administration and Boeing to participate, and we have three key objectives. The first is to, in fact, define the financial relationships amongst all the stakeholders. This is the first time all of the parties have sat down together to build a financial model that talks about the relationship in a free market economy.

The second outcome of the study is to make sure we all have a common understanding of the aviation security systems that we have in place so that we can allow the third element to go forward. When there are recommendations for changes in the system, we understand the financial implications so that we know the failures of each of the elements.

So, for example, if you want to increase the security tax on the flight tickets, we will know what the airlines will do. The flight data says we will have a reduction at the macro level in the number of passengers travelling. That has an impact on the airports and the airport fees that get charged, which has an impact then on what you do for future systems.

So from a recommendation standpoint, I believe that one of the things the Congress can do is help facilitate those discussions on a particular industry basis so that we really do understand the financial relationship and the security systems. I think as the captain pointed out, in the ideal world, we really would like industry to understand their responsibility, since we in industry own most of the infrastructure, the challenge we and the industry have is thus far a financial model has not included the cost for implementing the security requirements that now are really becoming fundamental to our society.

Ms. GRANGER. [Presiding] Mr. Cardin.

Mr. CARDIN. Thank you, Madam Chair. I really want to follow up more on what the Department of Homeland Security could be doing to encourage the best practices and technology development for homeland security using a lot of the technology that you have all talked about.

I represent a community where the port of Baltimore is located, and prior to September the 11th, we were inspecting somewhere around 2 percent of the cargo containers that came into the port of Baltimore. We are now probably up to around 8 or 9 percent. So the vast majority of our containers are not physically inspected as they come into the port of Baltimore. That is not unusual. The

technology that you have all talked about today would certainly help us in that effort to make the port safer and the containers better understood. It certainly would help in the intelligence aspects as to where we should be putting our efforts with the limited resources that are available.

So I am interested in the technology that has been talked about as to how quickly that type of technology could be employed.

I use the comparison with the airline industry. The airline industry wouldn't tolerate such a low amount of physical inspection. You feel very vulnerable if that was the case. But getting containers, which has been pointed out by the witnesses that you can—it is not difficult to get a container onto a vessel, and it could cause all types of harm. Our objectives, of course, are to inspect offshore, not—before it gets to the United States, but if it has been opened or tampered, that is the inspection at the port of—where it was loaded may become irrelevant.

So I guess my question to you is as a—as private sector individuals who look at the free market, who have certain interests in the bottom lines of your company and you want to make sure it is profitable, but also are very concerned about the security of our country, what should the Department of Homeland Security be doing in order to encourage industry to use best practices to get that security information encouraged by the government and to make this work to get these systems in place as quickly as possible? What should we be doing that we are not doing, Captain?

Mr. SALLOUM. The same question, sir, has been asked of us when we are meeting with the Belgium government, and they liked when we said that the security burden should not be on the shoulders of the government or on the port itself alone. Rather, to make this happen, we need the participation of everybody involved in the flow of the shipment. What does that mean? There are private sectors, and to have their involvement, the very simple and key element is to give them commercial benefits. Savings, increase their— this is the best incentives that you can have the private sector to participate in this system. So that is a key, simply put.

Mr. CARDIN. Mr. Katz, you didn't raise your hand, but I want to get your response, because we haven't solicited your assessment on infrastructure. I understand that because of the industry that you are in, but you are doing the technology that could be modified to meet the objectives that I have in regards to containers in the port of Baltimore on our security issues. So why aren't we consulting you more?

Mr. KATZ. Well, the technology exists today from a chip point of view. It does require integrating, and a considerable amount of software and interaction with the rest of the infrastructure, and that is independent of the chip. So I am not sure that—.

Mr. CARDIN. From a financial point of view, that is not going to be done, I assume. I assume we are not going to put—that that chip will not be put on every container in this Nation. We won't have the software in—we won't have the centers, et cetera. It is not going to be done, unless the Department of Homeland Security, the government, makes a decision that this is technology that we want to make mandatory in use of container security in this country, isn't that correct?

Mr. KATZ. That is correct, and I would point out another parallel situation. The State Department is going into a program to put the same sort of chips I described into passports. They have made an incentive to let all the rest of the world get on that program as well. Anybody that wants to be on the visa waiver program must have such a passport. So we could have anybody that wants to be on the cargo waiver program get on a technology program. That is something that the Department and the diplomats should be able to negotiate.

Mr. CARDIN. That is my point. I think that unless we have a strong governmental role here, that the free market itself, even with sensitivity on security, which it is clearly there, no question about it, it won't move forward, and that is why I guess it is a little frustrating as to what we can do to speed this thing up.

Mr. STEPHENS. Congressman, if I can, I think that the C–TPAT program and the wise investments that Congress has made in Operation Safe Commerce are great opportunities to see what the systems can look like, and then based upon that Congress in its wisdom can then look at the appropriate regulations, because I do believe that one thing that gets industry motivated are, in fact, incentives and the notion of being able to have a green lane to be able to move cargo through because you have met all the requirements for free entry; you have verified the integrity of those shipments moving on through. I think those are great programs that Congress can then help provide the pull that industry will get behind to deploy chips and systems like Mr. Katz is talking about that verify the integrity and allow you to move freely, because from our standpoint, it is about time and money and about being able to move commerce freely and efficiency the best way possible, recognizing we now have this new layer of security on.

And the government is the best one to understand the threat and what worries we have to make sure we respond to, but putting those incentives in I think are exactly the right areas to go. But I think OSC and C–TPAT are going to give you all some good sense, and so my presumption is you all look very closely at how the investment that you are making in OSC will play out over this next year.

Mr. CARDIN. Thank you. I think the visa waiver analogy is a good analogy.

Ms. GRANGER. Before I call on Mr. Markey, let me say that we are going to have a series of votes in just a few minutes. It is going to be a very long series. So this will be the last question that we will be able to ask. Because I think we are going to be on the floor for an hour or two hours.

Mr. Markey.

Mr. MARKEY. Thank you. Mr. Stephens, in your testimony you explain that Boeing applied its best practices knowledge to the airport security problem. I was struck by the portion of your testimony where I don't describe Boeing's efforts in this key security area. Quote, the government selected Boeing to accomplish what many consider to be an impossible job, help Americans feel more secure about air travel by meeting a congressional mandate to screen 100 percent of checked baggage by December, 31, 2002 at all our Nation's commercial airports. Many experts thought the job

was not possible, but we accomplished that goal by building a world-class team and working hand in hand with our customer, the Transportation Security Administration and the aviation industry.

In less than 6 months, Boeing led the effort to install 6,000 explosive detection systems and explosive trace devices at 439 commercial airports around the country.

Now, as you may know, cargo that is shipped aboard passenger airplanes amounts to 22 percent of all cargo shipped in the United States, and currently none of that cargo is screened before it is boarded on to passenger airplanes.

My question to you is we have kind of got this cargo conundrum now, and many people are saying, oh, it is impossible to screen cargo before it goes onto passenger planes.

So I would ask for your comment on that, given the experience which you had at Boeing with the baggage check problem.

Mr. STEPHENS. Sir, I certainly believe that the technology is available. It may not be optimal, but the technology is available to make that happen.

Mr. MARKEY. When you say it may not be optimal, what do you mean?

Mr. STEPHENS. Very similar to what we do with the passenger baggage screening. Had we had more time, we would have installed the systems inline in the existing baggage systems and would not have installed the majority of the equipment in airport lobbies.

Mr. MARKEY. But you could create the level of security that you have for bags.

Mr. STEPHENS. Certainly we could.

Mr. MARKEY. Is that what you are saying?

Mr. STEPHENS. Yes, sir, certainly we could. I think the challenge is who is going to pay and I think that is the issue that comes back from the aviation industry, in the implementation of passenger baggage screening, Congress funded taxpayer dollars to go implement that system and it is the same sort of issue that I believe the aviation industry faces on the cargo side, new requirement, not part of the current market situation, so they are looking and saying I have got a revenue trade versus an income trade, how do I do I go fund that? And so from an implementation standpoint, it is certainly implementable. It is a question of where does the funding come from.

Mr. MARKEY. So each time I get on a plane or you get on a plane, there is a little fee?

Mr. STEPHENS. That is correct.

Mr. MARKEY. That is then pooled in order to create the revenue that then pays for this security?

Mr. STEPHENS. That is correct.

Mr. MARKEY. So you are saying a similar kind of system would have to be set up for cargo using cargo as people, saying that each piece of cargo, they would—depending on the size and weight, et cetera, that there would be a fee that is much like you and I have to pay every time we get on and off a plane now.

Mr. STEPHENS. Yes, sir. And I believe there will be some impacts on the aviation industry about the level of cargo, because then the market will look and say, I have an additional fee to pay, and I have a decision to make of time value of money. Do I need it there

tomorrow, or for a lesser fee can I ship on another mode of transport? Could be over the rail, could be trucks to get there. And you will see that discussion going back—.

Mr. MARKEY. It doesn't have to be on the passenger plane which is leaving at 3:00 this afternoon. It could be on a cargo plane that is leaving tomorrow.

Mr. STEPHENS. No question about it. That is correct. So I think you will get some feedback from the airline industry saying by putting those rules in place, you may impact our revenue in an already challenging aviation environment, versus on the other side it is the free market economy that will settle itself out.

Mr. MARKEY. But the very same thing that a passenger might be trying to sneak on could be snuck on through the cargo right now that would pose the same threat to the plane in terms of an explosive, not in terms of taking over the plane, but in terms of if the passengers wanted to sneak on an explosive, the same thing could now happen, but without the screening on the cargo.

Mr. STEPHENS. There is certainly that threat, yes, sir.

Mr. MARKEY. Well, without screening, you are right. So from my perspective, I think that the big argument has been that the technology is not there, but the same technology that is used or similar technology for passengers today could be used for the cargo.

Mr. STEPHENS. I would argue the technology is there.

Mr. MARKEY. And whose technology is it?

Mr. STEPHENS. There are a number of companies that have technology. As you may be aware, the systems deployed today are made by envision and L3com, but, you know, part of our work, we are evaluating and working with the Transportation Security Administration, looking at some 30 other companies that are offering technology that not only meet the current requirements but could potentially enhance it.

Mr. MARKEY. Would the technology now purchased for cargo be better than the original technology that was purchased for passengers because it has evolved just in the 2 years since that whole process has begun.

Mr. STEPHENS. It has improved.

Mr. MARKEY. So it actually could be better perhaps than the totality of the passenger cargo today.

Mr. STEPHENS. Perhaps.

Mr. MARKEY. I thank the Chair. Thank you, sir.

Ms. GRANGER. Following up on that, Dr. Gould, have you used your formula concerning checked cargo?

Mr. GOULD. No, we have not.

Ms. GRANGER. Ms. Lee.

Ms. JACKSON-LEE. I thank the Chair very much, and I thank the witnesses with debate on the floor of the House, it allows us a little time to spend as much time as we like with the witnesses. But I thank you for your testimony.

Let me try to pose briefly two questions. One, refresh my memory on what technology you are now using for interline bags, unaccompanied bags. I know that there is technology there, and do you think we are at maximum capacity with technology to check unaccompanied bags that are going through our airports?

The other point is that just a couple of days ago we discovered that one of the contractors that the Homeland Security Department used—it was really the Transportation Security Administration—seemingly overbilled the government, I would say about $700 million since I work with them and they were supposed to recruit those employees that were utilized, or are being utilized by TSA. Give us a sense of how we can be guided not to be overwhelmed by the many gadgets that the government may look at to improve homeland security? What should be the litmus test that we should use to ensure that we absolutely get the best product for the dollar?

This is best practices, but what should we be looking at and what should be our litmus test? If all the gentlemen could answer that. I would ask the distinguished gentlelady if I could submit my entire statement into the record, my opening statement, and I will conclude with this point as a member of the subcommittee and to the ranking member, I believe that this is one of the more important committees, not by my presence on it but by the fact that we started on 9–11 with the idea of our borders being penetrated, whether it was by flight, whether it is by other means, we know that the penetration of the border either through food, meaning the transportation of food across borders, the transportation of people across borders, the transportation across arms is truly one of our greatest concerns, and so I appreciate this hearing and I appreciate the gentlemen in responding to my questions. I thank you.

Mr. STEPHENS. If I might from an aviation and checked baggage standpoint, it is x-ray technology—does provide three-dimensional views of what is in the passenger bags themselves.

Ms. JACKSON-LEE. And is that updated technology?

Mr. STEPHENS. It is updated technology because it comes in two forms. One is the technology itself, but also the software algorithms that are used to validate and check the bags, and there is an ongoing process to work that. As I mentioned earlier, there are additional technologies being evaluated to potentially enhance the ability to screen the bags, and that is part of an ongoing activity that TSA has that you through their laboratories up in Atlantic City.

Ms. JACKSON-LEE. Do you think there should be any litmus test for random displays of products from the private sector that the government may be looking at to purchase?

Mr. STEPHENS. I believe there are, in fact, many companies that the government is looking at on a regular basis, and I believe those involved in technology, particularly out of the technology—the chief technology officer would be prepared to walk through a number of details about all the technologies you are looking at, because we participate in some of those reviews. In my sense it is quite extensive. We get calls and I personally get calls on a standard of two to three calls a week of companies that are offering technology, and one of our roles as a lead systems integrator is to take those calls in, evaluate them. We have a fairly extensive process that we use, not only on the technology side but also with outside venture cap lists to get an independent view, and then based upon that we as one company make additional recommendations in the Department of Homeland Security to give them thoughts and insights about

what we think is appropriate, and how it might fit in the broader system.

Ms. JACKSON-LEE. Do you think there are procedures in place—thank you.

Mr. GOULD. I do have 30 seconds. So I think the large systems integrators are playing a vital role in place of government to sort through some of the competing technologies out there. In our report we suggest five basic criteria to guide that investment process. The first being obviously the compelling value of the security product or technology. The second being an awareness that the public feels that this is a problem that needs to be solved. After all, it is their money that we are spending. Thirdly, that it offers a unique or blocking technology. Fourth is the privacy issue, nonnegative impact on privacy. Certainly there is a lot of concern about that.

Chairman Cox mentioned earlier that balance between freedom and security. And finally, and perhaps most importantly from Captain Salloum's standpoint and others, nonnegative impact on operational efficiency. We believe that it is possible to construe good homeland security and competitiveness and flow of commerce as two components of the same objective function. We can be doing both. We ought to be doing both at the same time.

Ms. JACKSON-LEE. Thank you. Yes.

Mr. SALLOUM. Definitely tracking devices are important, and scanning is definitely also important, but I believe this is not it. What we need—as there is a lot of effort from the official side to protect our borders, I believe we need another source of information from the private sectors, and then we will have two sources of information so we can cross-check these data and then we can flag a specific shipment or enterprise. So the key is to keep doing what we are doing from the official side, but we need to encourage private companies to go—like we say, initially on a system like the airline industry system like Saber, but for the cargo. This will be a source of data for us so we can cross-check this data and flag the specific shipment and enterprises.

Ms. JACKSON-LEE. I thank you.

To the distinguished chairwoman, let me just say that this is an important hearing, and one of the things I am not sure whether the other members focused on that I hope we can discuss is the kinds of private security products, if you will, or individual security products—I am not talking about an alarm in your home—that many of our constituents are being bombarded with, and the question is whether homeland security engages in setting some kind of litmus test or helping analyzing of technology, because more and more individuals, communities, homes are looking to buy all kinds of gadgets that came about after 9/11, and I think it is crucial that as we secure the homeland, that we provide some sort of standards to guide those who are attempting to secure their families and their communities.

Ms. GRANGER. Thank you.

One short question, Ms. Sanchez.

Ms. SANCHEZ. Dr. Gould, you just mentioned in the list of four or five that you gave the number two was the public perception. Can you just expand on that a little bit, because as politicians, we are always looking at public perception, but it is interesting to hear

from your end that you think we should be investing in something that the public thinks is important when it may not be?

Ms. GRANGER. Very quickly. We have 7 minutes.

Mr. GOULD. Certainly. And in one minute, I absolutely do believe that that critical set of permissions that the media occasionally offers Congress as a set of permissions or awareness to identify the problem, to recognize that it is a problem out there, that there is a matching solution with it and sort of brick it into the deliberative process here in the Hill is actually a vital component of how small companies and medium-sized companies are trying to enter this mark. They recognize that your engagement on these issues is critical in making some of these new solutions a possibility in the market, because frankly the large systems integrators and others are buried.

Steve just—Rick just mentioned that he is bombarded, several calls a week. There is a tremendous volume of companies trying to break through that, and this is one of the ways that that can—.

Ms. GRANGER. Thank you. I am going to have to stop you now. I thank the panel for their testimony. There being no further business before the subcommittee, I thank our witnesses today. Our hearing is now adjourned.

[Whereupon, at 12:52 p.m., the subcommittee was adjourned.]

○