AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

TAX INCENTIVES FOR HOMELAND SECURITY RELATED EXPENSES

HEARING

BEFORE THE

SUBCOMMITTEE ON RURAL ENTERPRISES, AGRICULTURE, & TECHNOLOGY

OF THE

COMMITTEE ON SMALL BUSINESS
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

WASHINGTON, DC, JULY 21, 2004

Serial No. 108–75

Printed for the use of the Committee on Small Business

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

U.S. GOVERNMENT PRINTING OFFICE

96–551 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

COMMITTEE ON SMALL BUSINESS

DONALD A. MANZULLO, Illinois, *Chairman*

ROSCOE BARTLETT, Maryland, *Vice Chairman*
SUE KELLY, New York
STEVE CHABOT, Ohio
PATRICK J. TOOMEY, Pennsylvania
JIM DEMINT, South Carolina
SAM GRAVES, Missouri
EDWARD SCHROCK, Virginia
TODD AKIN, Missouri
SHELLEY MOORE CAPITO, West Virginia
BILL SHUSTER, Pennsylvania
MARILYN MUSGRAVE, Colorado
TRENT FRANKS, Arizona
JIM GERLACH, Pennsylvania
JEB BRADLEY, New Hampshire
BOB BEAUPREZ, Colorado
CHRIS CHOCOLA, Indiana
STEVE KING, Iowa
THADDEUS MCCOTTER, Michigan

NYDIA VELÁZQUEZ, New York
JUANITA MILLENDER-MCDONALD, California
TOM UDALL, New Mexico
ENI FALEOMAVAEGA, American Samoa
DONNA CHRISTENSEN, Virgin Islands
DANNY DAVIS, Illinois
GRACE NAPOLITANO, California
ANÍBAL ACEVEDO-VILÁ, Puerto Rico
ED CASE, Hawaii
MADELEINE BORDALLO, Guam
DENISE MAJETTE, Georgia
JIM MARSHALL, Georgia
MICHAEL MICHAUD, Maine
LINDA SÁNCHEZ, California
BRAD MILLER, North Carolina
[VACANCY]
[VACANCY]

J. MATTHEW SZYMANSKI, *Chief of Staff*
PHIL ESKELAND, *Policy Director/Deputy Chief of Staff*
MICHAEL DAY, *Minority Staff Director*

SUBCOMMITTEE ON RURAL ENTERPRISES, AGRICULTURE AND TECHNOLOGY

SAM GRAVES, Missouri, *Chairman*
BILL SHUSTER, Pennsylvania
SUE KELLY, New York
SHELLEY MOORE CAPITO, West Virginia
MARILYN MUSGRAVE, Colorado
PATRICK TOOMEY, Pennsylvania

[RANKING MEMBER IS VACANT]
DONNA CHRISTENSEN, Virgin Islands
ED CASE, Hawaii
MICHAEL MICHAUD, Maine
BRAD MILLER, North Carolina

PIPER LARGENT, *Professional Staff*

CONTENTS

WITNESSES

	Page
Hyslop, Mr. James, President, Standing Stone Consulting	3
Ducey, Mr. Ken, Markland Technologies, Homeland Securities Industries Association	5
Chace, Mr. Richard, Executive Director, Security Industry Association	7
Orszag, Mr. Peter R., The Brookings Institution	9

APPENDIX

Opening statements:	
Graves, Hon. Sam	27
Prepared statements:	
Hyslop, Mr. James, President, Standing Stone Consulting	28
Ducey, Mr. Ken, Markland Technologies, Homeland Securities Industries Association	32
Chace, Mr. Richard, Executive Director, Security Industry Association	37
Orszag, Mr. Peter R., The Brookings Institution	42

TAX INCENTIVES FOR HOMELAND SECURITY RELATED EXPENSES

WEDNESDAY, JULY 21, 2004

HOUSE OF REPRESENTATIVES
SUBCOMMITTEE ON RURAL ENTERPRISES, AGRICULTURE AND TECHNOLOGY
COMMITTEE ON SMALL BUSINESS
Washington, D.C.

The Subcommittee met, pursuant to call, at 10:05 a.m. in Room 2172, Rayburn House Office Building, Hon. Sam Graves, presiding.

Present: Representatives Graves, Shuster and Velazquez.

Chairman GRAVES. Good morning. I would like to welcome everybody to the Subcommittee on Rural Enterprise, Agriculture and Technology.

Today's hearing is going to focus on H.R. 3562, The Prevent Act, introduced by my colleague, Representative Shuster.

In today's post-9/11 world, businesses need to take precautions against the possibility of a terrorist attack. However, it is oftentimes very expensive to secure business against the possibility of a terrorist attack. Businesses must outlay a great deal of capital to guard against any terrorist activity. Moreover, what is the likelihood of a terrorist attack against a specific business? It is probably pretty small. However, no one can say for sure what the next target is going to be.

Besides the terrible human lost suffered on September 11th, our economy suffered terrible losses as well. We must safeguard the livelihood of people as well as their safety.

H.R. 3562 provides an incentive to businesses through tax credits. I think it is one of the many ideas that needs to be looked at in order to safeguard the population and our economy.

[Chairman Grave's statement may be found in the appendix.]

I am now going to turn to Ms. Velazquez, the ranking member of the full Committee for her opening remarks.

Ms. VELAZQUEZ. Thank you, Mr. Chairman.

The events of 9/11 force us to chart a new course for the future of our nation. One focus on how to better protect America. This plan requires us to spend ever-increasing amounts of money to protect and preserve our country. Today's hearing will provide us with a forum to explore opportunities in an effort to make America's small businesses and the general public at large more secure.

We will examine the different needs of small firms as they struggle to pay the high cost associated with securing their companies. Security measures in place have increased dramatically in the last three years, but still it is a concern that more needs to be done.

Protecting America's infrastructure and its businesses must involve a public/private partnership. The federal government has an interest in ensuring private firms put homeland security measures in place. It provides a benefit to not only the firms but to the broader public. The costs of a terrorist attack are simply too high. They extend well beyond business owners themselves, and affect our entire nation.

It is for this reason that protecting the homeland should not be a government alone effort. Unfortunately, given the budget deficits of nearly $450 billion, we simply do not have an infinite amount of money to spend on homeland security. It means Congress must pinpoint where security is lacking, and provide incentives for our nation's businesses to bolster.

Because of the fiscal situation we are in, it is necessary to look at all available options to ensure we encourage investment in security where it is needed most. Tax incentives are clearly an option, but they cannot be the only one.

In crafting a solution, it is necessary to explore the delicate balance between a firm's decision to invest in homeland security and other costs of doing business. Encouraging firms to spend on security for the mere sake of doing so does nothing to increase homeland security and only hurts the bottom line for the U.S. businesses. The government must also have a role in determining how homeland security money is spent. This would allow us to better identify ways to reward businesses that devote resources which not only protect their companies but their communities as well.

As part of this effort, we also can improve the coordination between local, state, and federal law enforcement officials and the private sector, and whatever solutions are put forward today, they must address the needs and concern of small businesses.

After working closely with the small business community for many years now, I know these firms simply do not have infinite resources to invest in high-tech security equipment and security personnel. I truly wish the federal government had more money to spend on homeland security, to provide the safest environment for our citizens and our nation's 23 million small businesses. Unfortunately, we are in a position where difficult decisions have to be made.

It is important that we provide the best policies to protect our citizens and our businesses. Not only is it a good security policy, but it is sound economic policy.

Thank you, Mr. Chairman.

Chairman GRAVES. Thank you, Ms. Velazquez.

Representative Shuster.

Mr. SHUSTER. Thank you, Mr. Chairman, and I appreciate the opportunity to have this hearing, and I want to welcome our witnesses here today.

I believe that homeland security is one of the most important issues that we face on a day-to-day basis in our country today. The

times have changed, and the post-September 11th world companies are raising a host of new questions about security.

It was events of September 11th that have shown us how quickly those who wish to do us harm can affect our lives and the economy of this nation. In fact, many companies are taking the initiative to secure their workplaces, realizing that no longer can we have an open-door policy at our businesses and corporation.

But just as many are trying to do more, many are doing nothing at all. More than 75 percent of the scores of U.S. firms that hired international security company Kroll to promote security upgrades after September 11 attacks, never implemented the recommended improvements.

Recently, I introduced legislation, the Prevent Act, to provide incentives for businesses to further their efforts in securing workplaces. The legislation amends the tax code to provide tax credits to businesses that take the initiative to install building security devices, take part in security analysis, or create business co-location sites.

It is not just putting a camera on a wall and believing that we have taken a step towards security. It is much more than that. It is a need for a security plan, analysis of potential weaknesses, and understanding that this process will become more involved, not less.

In an open society it is difficult, but not impossible, to shield our workforce and our business infrastructure from harm. It is imperative that we provide incentives for businesses to take proper security precautions. This legislation provides a needed boost towards protecting our workforce and economy.

I do not believe that additional burden of government regulation is the correct way to approach this problem. Our business people know the level of threat to their own businesses, and it does them no good to set static guidelines from government. In fact, the Director of Worldwide Security for Texas Instruments has in the past said, "Let us as a business decide best to protect our business."

Again, thank you, Mr. Chairman, for holding these hearings today. I want to welcome the witnesses again, and I would especially like to give a warm welcome to Jim Hyslop from Standing Stone Consulting. He is from Huntington, Pennsylvania in the 9th Congressional District of Pennsylvania, and appreciate your participation here today.

Chairman GRAVES. I do want to welcome all the panelists here today, and the way we run the format is everybody has five minutes to give your statement, and the lights will come on. When you have one minute left, the yellow one will come on. But it is not—you know, if you go over, it is not that big of a deal. But I do want to make sure that all statements of the members and the witnesses will be placed in the record in their entirety.

I too, would like to welcome James Hyslop who is the President of Standing Stone Consultant today, and we will go ahead and start with you if that is alright.

STATEMENT OF JAMES HYSLOP, STANDING STONE CONSULTING

Mr. HYSLOP. Thank you very much for the opportunity to participate in this hearing. As you know, my name is Jim Hyslop. I am the CEO of a small security consulting firm based in Huntington, Pennsylvania. I deal with both small and large companies that are trying to improve the security of their workplace and their workforce.

Small businesses and other small organization managers must decide how to allocate their precious resources. Often security planning and implementation is like buying insurance, a hedge against a probable event. Something bad may happen but then again it may not.

When resources are scarce, managers are forced to opt for placing their money where it will provide a good return. Most of the time this is okay, but when it is not, it usually means catastrophe for the business and frequently puts the general public in danger as well. Exploding bombs, biological agents, and other treats do not discriminate in their target selection.

Our experience after hundreds of security assessments is that most organizations do not have a security strategy or plan. We see the use of security tactics that may or may not be appropriate for their intended purpose. There is no underlying plan of how these tactics should be used. All too often the money spent on these tactics is wasted.

I believe it is good policy for the government to provide financial incentives to small businesses and organizations to plan and execute a security strategy. Without such an incentive it will not get done, and that puts all of us more at risk.

The introduction of legislation such as The Prevent Act sponsored by Congressman Shuster is an important step forward towards the government taking a more active role in this effort.

The assessment process is the basis of security planning. It determines where you are now and allows you to set and prioritize reasonable goals for where you want to be in the future. Assessment identifies the assets, the people, and the processes that need protection. It also identifies the probable threats that these assets may face and how they are vulnerable to those threats.

The consequence of a carried-out threat is the risk the organization faces. Once risk is understood, a plan can be developed to mitigate them. Qualified security professionals have the knowledge and experience to guide the planning process so that it will work in the culture of the business. All tactics do not work equally well in all situations. Security planners understand how tactics can and should be used to effectively mitigate the risks.

Once there is a plan and the appropriate tactics have been determined, the implementation can then be managed by the business owners.

Again, our experience has been that the difference between strategy and tactics is rarely understood. Too often there is no clearly stated security goals and no way to measure if any progress is being made.

Clarify the difference between strategy and tactics. Security strategy is a plan to achieve the desired goals while tactics are those actions taken to achieve the goals. Tactics are ultimately chosen to modify behaviors by deterring, detecting, delaying, and deny-

ing the ability to behave inappropriately. Strategy is determining what types of behaviors you wish to discourage, and often which types you wish to encourage.

During an assessment, vulnerabilities and behaviors are identified from which strategies are developed. Only then should tactics be selected to produce the desired behaviors.

For example, closed circuit television, CCTV is a popular security tactic, but how does CCTV deter, detect, delay, or deny? CCTV is basically an investigative tool. It watches and can record activity, but it does not respond to what is seen. An asset that is being protected requires an immediate response to a threat, and CCTV alone is not an appropriate tactic. It must be supported with other tactics and other procedures.

Equipment manufacturers often offer free assessments but you always seem to need the equipment they are selling, be it cameras, card-readers, guard services or whatever. Equipment is installed without a clear understanding of what it can and cannot do, and it often provides a false sense of safety and security. This can cause people to let their guard down by relying on technology to do things it really cannot do. The result is that you may actually be more at risk.

No security plan is 100 percent effective, but being 90 or 95 percent effective is a great improvement over where we are now. The point is without an assessment and a strategy we frequently waste money on tactics that do not deliver the expected results.

Thank you again for listening to my statement.

[Mr. Hyslop's statement may be found in the appendix.]

Mr. SHUSTER. [Presiding] Thank you, Mr. Hyslop, and now we will hear from Ken Ducey who is the President of Markland Technologies, and he is representing the Homeland Securities Industries Association.

Good morning, Mr. Ducey. Please proceed.

STATEMENT OF KEN DUCEY, MARKLAND TECHNOLOGIES, HOMELAND SECURITIES INDUSTRY ASSOCIATION

Mr. DUCEY. Thank you. Representative Shuster, Representative Velazquez, it is a pleasure to appear before you today. Accompanying me today is Bruce Aitken, President of Homeland Securities Industry Association, the HSIA.

The HSIA was organized in November 2001, and formally launched over a year ago. We have over 400 members, ranging from multi-billion dollar defense contractors to mid-sized firms and incubator firms.

In my oral presentation today, I will summarize the views and recommendations of HSIA. The association's views represent the consensus of HSIA members, but not the particular views of any one member.

In general, HSIA strongly supports legislation such as H.R. 3562, to provide tax incentives to promote private sector homeland security initiatives.

Since 9/11, America has begun a fundamental transformation from an open society to one that must continually weigh the secu-

rity of its citizens and corporate assets from terrorist attack. In the immediate aftermath of 9/11, the administration and Congress acted with vigor.

Unfortunately, partisan politics in the Legislative Branch held up rapid increases in HLS funding, and that Congress did not release Fiscal Year 2003 funding until nearly halfway through the 2003 fiscal year. This meant that the substantial increases in HLS funding that had been anticipated in the fall of 2002 for the first responders and others did not begin to be released until 17 months ago.

Since then the administration has moved quickly but first responders and others involved in HLS still have many needs for which funding has just begun. As a consequence, it is understandable that frustrations have been felt among first responders throughout the country, and among the companies who hope to serve them, including the HSIA members.

America is an open society. That is the strength of our democracy and the source of all our vulnerability. Two years ago on the first anniversary of 9/11 the Washington Post analyzed America's vulnerability to terrorist attack and gave an overall grade of C minus for HLS. Of course, this is unacceptable.

America faces a challenge which is likely to take years to accomplish. Therefore, we repeat a call we made in congressional staff briefings in January and February 2003 for an end to partisanship in HLS.

Our concerns about the HLS fall into three categories: One, federal procurement; two, state and local procurement; and three, private sector initiatives.

With respect to federal HLS procurement by DHS and other federal agencies with related procurements, we believe that the administration has done a commendable job in successfully launching the new department in a very short time, as well as in meeting its deadline to federalize airport passenger and baggage screening. In addition, we commend the department for its so-called "Industry Days."

DHS has gone to great and commendable lengths to outreach to the federal contracting community to share with firms DHS's vision, acquisition plans, and updates about its programs.

However, we have communicated with Congress in other hearing constructive suggestions to help improve this system in the future. We believe that the incidents of sole-source contracts and sole-source delivery orders off the GSA schedules should decrease.

Today we address the need for tax incentives for homeland security-related expenses. In the April 6, 2003, Sunday New York Times an article appeared with predicted that by 2008 annual HLS spending would increase from the 2003 annual level of about 60 million to 200 billion annually, and the article predicted that two-thirds of this spending would be in the private sector.

Yet the best estimates that we have seen suggest that since 9/11 private sector spending for HLS has increased only four percent.

The HSIA worked with a group organized by the American National Standards Institute, ANSI, from January 2004 to May 2004. The purpose of this group was to develop a recommendation for the 9/11 Commission, to help promote development of voluntary private

sector HLS standards. We accomplished this and made a recommendation that NFPA Code 1600 serve as a model or framework for HLS private sector standards.

This led to a discussion about how to educe the private sector to invest in HLS measures and equipment. This is a crucial issue since the vast majority of U.S. critical infrastructure is privately owned.

The consensus of our group, which included over 40 organizations, was that the 9/11 Commission should recommend to Congress tax incentives not only for private companies investing in HLS initiative, but also for municipalities.

In conclusion, we strongly support the Subcommittee's efforts on this important subject. We would be happy to answer any questions. Thank you.

[Mr. Ducey's statement may be found in the appendix.]

Mr. SHUSTER. Thank you, Mr. Ducey.

Now we will hear from Richard Case, the Executive Director of the Security Industry Association. Mr. Chace.

STATEMENT OF RICHARD CHACE, SECURITY INDUSTRY ASSOCIATION

Mr. CHACE. Good morning, Chairman Graves, Ranking Member Velazquez, Congressman Shuster, and other members of the Subcommittee.

Thank you for giving me the opportunity to participate in this important hearing on tax incentives for homeland security-related expenses, and in particular, H.R. 3562, The Prevent Act that was introduced by Congressman Bill Shuster.

My name is Richard Chace, and I am the Executive Director and CEO of the Security Industry Association, and it is my honor to testify today on behalf of the Security Industry Association, SIA, which represents over 700 electronic security equipment manufacturers, distributors, and service provider organizations around the country and throughout the world.

For more than 30 years the Security Industry Association, a nonprofit international trade association, has represented electronic and physical security product manufacturers, specifiers, and service providers. As an association our primary mission is to promote growth, expansion, and professionalism within the security industry by providing education, research, technical standards, and representation in defense of its members' interests.

The member companies of our association employ roughly 150,000 plus individuals. While this is a sizeable constituency and a fraction of the industry as a whole, the majority of our members employ roughly 500 employees or less.

This, according to the U.S. Small Business Administration, is the definition of a small business, and it is indicative of the significant number of security industry companies' employees that are affected by small business laws and regulations.

It is because of our industry's vulnerability to the effects of small business laws and regulations that the Security Industry Associa-

tion is in strong support of H.R. 3562, the Prevent Act, as introduced by Congressman Shuster.

We applaud Congressman Shuster's leadership in introducing this critical piece of legislation. We would also recognize Congressmen Weller and Crowley for their collective work and focus in this area in past sessions.

Given the increased focus on the private sector's role in homeland security, and the many economic benefits that can arise from appropriate security applications, it is vital that private sector businesses are given the tools needed to properly secure employees, customer, and important assets.

Passage of Congressman Shuster's legislation, H.R. 3562, would be a major step in promoting the private sector's in meeting the post-September 11th challenge of adequately securing the homeland. This important bill provides appropriate tax incentives for businesses to enhance their security while simultaneously promoting safety for employees, customers, and enhancing productivity.

In today's uncertain world, the private sector and the government need to work together to provide a more secure environment for places such as malls, movie theaters, stadiums, hotels, apartment complexes, and other areas. H.R. 3562 would provide the necessary incentive for businesses that wish to apply state-of-the-art security technology to protect our local restaurants, businesses, movie theaters, and other soft targets.

Last year Congress passed, and President Bush signed into law, the Jobs Growth Tax Reconciliation Relief Act of 2003, H.R. 2, which allowed for an increased amount, up to $100,000 for tax expenses as well as an increase in the bonus depreciation from 30 percent to 50 percent. This increase allows especially small businesses the opportunity to upgrade or purchase security systems if they so desire.

This, in turn, helps to sell these products and helps more than half of our membership. These tax breaks are a win/win situation for the customer and the manufacturer, while working to infuse more capital back into the economy.

This legislation runs out as of January 1, 2005, and the ability to incentivize small businesses and their assets will be lost. These provisions act as a cost-effective tools that will help America's businesses play an increased role and enforce multiplier in homeland security.

As continuing concerns of security issues place economic strains on consumers' businesses, a reliable security infrastructure has become essential in keeping businesses vibrant.

In a GAO report released on Friday entitled "Status of Key Recommendation," GAO has made to DHS and its legacy agencies. It calls for actions to be taken by the Department of Homeland Security.

In the national strategy for homeland security released by the administration in July of 2002, one of the recommendations was to determine the need for security regulations, grants, or incentives for securing critical infrastructure. This has not been done, and H.R. 3562 would play a critical role in successfully reaching this goal.

To help support the Department of Homeland Security's regulation and recommendation development, standards development should not be overlooked. In recent years, Congress has passed several laws making it clear that federal agencies rely upon private and voluntary standards whenever feasible; namely, that all federal agencies and departments shall use technical standards that are developed or adopted by voluntary consensus standard bodies.

Using such technical standards is a means to carry out policy objectives or activities defined by the agencies or departments.

The SIA supports the standards development effort, which is beneficial to small businesses and the small business end user. In the case of procurement and internal operations, end user is the role the government takes. As users the government has the opportunity through standards to resolve technical problems, to make security products work together and share lack of confusion in the marketplace, and share the interoperability of products and specify the responsible use of security technologies.

Security systems and security technology applications, when utilized in the context of clearly defined policies, provide a wide range of benefits, especially to the corporate bottom line. Sophisticated and well-planned security applications in a corporate setting provide a significant return on investment. They play a role in the activity of business and should not be seen as an expense or drain.

In conclusion, I would like to once again this Subcommittee for holding this hearing. It is my hope that this initial conversation will spark greater interest in 3562, and serve as a springboard for Congress to enact this legislation.

As the executive director of SIA, I would like to offer my association and its members as a resource for this Committee and the Congress as you grapple with these difficult homeland security-related issues.

Chairman Graves, Congressman Shuster, thank you for your attention to this matter, and I will be happy to answer any questions that you or your colleagues on this Subcommittee may have of me. Thank you.

[Mr. Chace's statement may be found in the appendix.]

Mr. SHUSTER. Thank you, Mr. Chace.

We will now hear from Peter Orszag, did I pronounce that right?

Mr. ORSZAG. You did.

Mr. SHUSTER. Okay. He is from the Brookings Institute. Go ahead and proceed, Mr. Orszag.

STATEMENT OF PETER R. ORSZAG, THE BROOKINGS INSTITUTION

Mr. ORSZAG. Thank you very much for having me here this morning, and I am particularly encouraged that your legislation and my co-panelists have recognized the need to alter the incentives facing private firms in the area of homeland security because, in my view, this is one of the greatest short-fallings in our homeland security efforts to date, which is that we have not tackled the

problem of how to alter the incentives facing private firms. Just leaving it up to the market itself without any change in the incentives is not going to work.

So the key question is how we should change those incentives, and certainly tax credits are one way of doing so. But we do need to realize the shortcomings or problems in tax credits. Any approach to altering the incentives will have problems, so this is not necessary definitive to say that tax credits have some problems, but let me just walk through some of them, and in my view actually, they are substantial enough to prefer an alternative approach.

The first problem with the tax credit is that it can educe gold-plating; that is, especially when there are products that are useful for homeland security purposes but for other purposes one can educe excessive spending on those products.

For example, your legislation includes things like door locks. Door locks have some homeland security benefits, but they also protect against vandalism, against theft, and other more private sector-oriented types of activities. By decreasing the cost of certain types of products one can educe excessive spending on those kinds of products because the firm is not facing the full cost.

Another related problem is that a tax credit tends to buy out the base of activities that firms were doing anyway, so for firms that were already spending X hundred dollars on homeland security activities, we now have a cost to the federal government in response to no change in their activities. In other words, it is not a marginal incentive, it is not for something that is just new activity. It would buy out the base of any activity that would have occurred anyway.

The third problem is that tax credits do not do a particularly good job of sorting risks in the sense of across sectors. I worry a lot more about the security of our chemical facilities than I do about remote shopping malls at various parties of the United States simply because the opportunity for terrorist harm varies substantially, yet the tax credit approach provides the same benefit to putting in a door security system at a shopping center in the middle of a remote area as it does in a more high profile chemical facility.

Fourth, and I think this is a very substantial problem, our tax code is extremely complicated. Complexity has increased markedly over the past several decades, and implementing an approach like this can prove to be very difficult. For example, the legislation says that computers used to combat cyber terrorism will be eligible for the tax credit.

I have no idea how the IRS will judge whether a computer is used to combat cyber terrorism or for any other purposes, and once we start getting into that kind of ambiguity, that is where we get complexity.

The fifth point is the fiscal outlook. The nation faces a long-term fiscal gap of between seven and 10 percent of GDP. It is a massive long-term fiscal problem. Tax credits will, unless they are offset through other revenue or spending changes, exacerbate that fiscal gap.

For example, the bonus depreciation in Section 179 provisions that were already mentioned this morning, if extended over the next 10 years would cost about $475 billion on top of an already

fairly dismal fiscal picture. I do not know exactly what the score is for this legislation, but it certainly could be nontrivial.

And then I think finally, and most fundamentally, there is sort of a philosophical question, which is who should bear the cost. Tax credits spread the cost of homeland security investments across the tax-paying population as a whole. Some people may view that as fair. This is a public good that we are providing, protecting against terrorist attacks. Other people may view it as unfair. The rest of the population is effectively subsidizing those firms or occupants or people who are engaged in the riskiest activities from the point of view of exposure to a terrorist attack.

Beside the fairness argument, I do not want to fully weight into those, there is an incentive point. By spreading the cost over the whole population rather than concentrating the cost on the stakeholders involved you are losing the incentive effect of minimizing or at least reducing the most dangerous activities.

If instead the stakeholders pay, they bear the cost, and normal market forces would then tend to diminish the most dangerous activities, and from a society's point of view that is actually exactly the right outcome.

I see that I am running out of time so I will not go into full detail on some of the alternatives, but I do think that there are market-based, market-friendly dynamic systems that could be put in place that are not tax credit-based, that do not worsen the fiscal outlook, and that do not spread the costs over the whole population as opposed to the stakeholders, and I would be happy to answer questions about them.

But let me just reenforce the basic point, which is I think it is absolutely essential to be looking at ways of changing the incentives facing private firms. We have not tackled this problem. It is very difficult to do. Perhaps you and I have somewhat different views on this specific proposal, but the basic idea of trying to tackle this problem is one that I think is crucially important, and I commend you for taking a step in that direction. Thank you very much.

[Mr. Orszag's statement may be found in the appendix.]

Mr. SHUSTER. Thank you, Mr. Orszag, for your testimony, and there is only two of us here so what I thought we would do is go back and forth five minutes, five minutes, and I have a couple of questions I will start off with, and then yield to the ranking member.

Mr. Hyslop, you had mentioned the need for security devices but also a security plan. Can you tell me a little bit more about what it looks like to go in, and what the plan entails when you go and do this analysis?

Mr. HYSLOP. Security planning is—I will give you the very short, simple version. It is assets plus threats plus vulnerabilities equal risks.

Remember in my statement I said the risks are the consequences of the threat being carried out.

So, for example, let us say we have a business and it has a vital database that is critical to the ongoing function of the business. That computer then that houses that database needs protection. So

we look at—that is the asset, the computer and the data that it contains.

All right, how do we protect that? What are the threats against it?

Well, the threats could be it could be hacked or it could be physically damaged. So we look at those threats against that asset. How is this particular asset vulnerable to those particular threats in this particular business. That is what I meant when I said within the culture of the business.

Let us say, for example, that this business is open to the public. People have to come and go, so you cannot keep people out of the business to protect this computer. What do you need to do? Perhaps in that case what we need to do is have a redundancy, a computer offsite somewhere so that the data and that computer can be protected so that if something does physically happen or that computer that is in the business is hacked, you have this other one as a backup. You can put it in place and the business can continue.

We have had—I do not want to go into a lot of detail the threats that businesses are facing, but there are privately-held water companies, for example, that are controlled by systems called SCADA systems. Those are all computer-controlled.

How do you protect that computer and that database? It is critical to how that water system functions and how we would all be protected if something threatened that water system. So that is the kind of thing—in that case, you know, they do not have a lot of public access. You could protect it in different ways. That is what I mean by you have to work within the culture.

Mr. SHUSTER. As Mr. Orszag mentioned about cyber—a computer that protects against cyber invasion, can you tell the difference or is there different devices, different software that protect against, or is it no clear-cut? I am not familiar.

Mr. HYSLOP. Well, certainly if you had a redundancy, if it was my business and I was setting up a computer to have redundant information available if somebody hacked into my primary system, I do not think there is any question of why you bought that computer.

Mr. SHUSTER. Right.

Mr. HYSLOP. And we do work with firms that ask that question. What happens to my information while it is in your system? I need to tell them that, well, this is how I protect it, and this is what would happen if we were under attack.

Mr. SHUSTER. Right.

Mr. HYSLOP. So I think there may be some cases where it is not very clear, but I think in most cases it is going to be—

Mr. SHUSTER. Stores obviously—

Mr. ORSZAG. Yes, if I could just comment on that. I mean, let us take auxiliary systems for example. Auxiliary systems can provide benefits against cyber attack, but they also provide a variety of just normal business interruption, you know, for a reason entirely unrelated to cyber attack, the local grid goes down or there is some other problem. Having auxiliary systems in place provide a continuity to business operations that have nothing to do with terrorist attacks.

So I actually think that provides a good example of dual use types of activities that it is very difficult to sort of draw a line and say this is just for homeland security.

Mr. SHUSTER. Right. A question for maybe all of you in your experience, maybe just go down the line there. Why are not companies investing in homeland security? Is it because of the cost mainly or is it because of belief that they are not at risk? Just going to go down, what is your experiences? Could you briefly touch on that?

Mr. HYSLOP. My experience is it is basically cost. There are other factors, but as I said in my opening statement, most particularly small businesses have to look at the return on the investment, and it is like buying insurance. Most of them do not believe that something bad is going to happen, and most of the time they are right. But in that one or two occasions where they are wrong it is catastrophic.

Mr. SHUSTER. Right.

Mr. HYSLOP. And it is not only catastrophic to the business, it can be catastrophic to the general public at large. If one of those chemical plants is attacked—

Mr. SHUSTER. Right.

Mr. HYSLOP. —it is not just going to be the people that work there, it is going to be the people in the surrounding community. And I am from a rural community. I take a little offense at someone saying a rural mall is not all that important. To me it is just as important as that chemical factory in Bayonne.

Mr. SHUSTER. Right. And that chemical factory in Bayonne is going to affect people all across the country because of the supply and what have you.

Mr. HYSLOP. Right.

Mr. SHUSTER. Mr. Ducey, do you care to—

Mr. DUCEY. Yes, I think it is a combination of both. I do not think that either—even if it was free right now, I do not think there is a lot of incentive for companies to implement different homeland security plans just because, as you said in your opening

statement, everybody thinks, well, what are the chances of it actually happening to me.

I think it has got to be not just incentives but also sort of like a media campaign that basically suggests that, you know, workers coming to work every day are at risk unless you take a certain initiative on behalf of your employees, and then from that obviously employees may will go work for a company that has taken initiatives because they know they are going to be safer going forward.

Mr. SHUSTER. Right. Mr. Chace?

Mr. HYSLOP. Can I just back in with just one comment?

Mr. SHUSTER. Sure.

Mr. HYSLOP. One of the things I have seen when we talk about planning, you sit with a business owner and you say you need to think about the consequence of this risk in terms of dollars and human casualties. When you do that you are really taking people out of their comfort zone.

I think one of the reason they do not like to think about this is because when they are forced to think in those terms it becomes a much more serious situation.

Mr. SHUSTER. Right. Mr. Chace.

Mr. CHACE. Yes, I would like to comment on one thing that my colleague over here mentioned.

There are fringe benefits to these systems. Of course there are. And it would be a waste of the resources to have it only apply to homeland security. That would be irresponsible. If you are going to make that investment, you darn well better have some ancillary benefits to it. I just want to make sure that is understood as well.

But let me talk in terms—we need to take a crawl, walk, and run approach here. Security is very subjective. What is security to you might be a dog and a fence. What is security to me might be high access control system and a perimeter guard.

So it is a very difficult thing to legislate. It is also extremely difficult to get our hands around it to define. So that being said imagine how much more difficult it is for the small business or the private sector to say, well, what is my real risk here? You have to take in geographic locations. You have to see is it just my assets that I need to worry about securing? Or do I need to worry about that I am located five miles away from a nuclear power plant even though I am just a small business?

Those are all things that go into determining what type of security system you need. So what I advocate and what our associate advocates is the fact that you need to have clearly defined policy that says this is how you use and begin to look at security. It is a tool in your toolbox. It is one piece of a total solution for security. It is not the solution.

I think the biggest misnomer as we move forward thinking that technology is going to solve the problem. It is not going to because a nice, big CCTV system is totally useless if there is not a good pol-

icy defining how those people are going to be using it, what it is going to be used for, who is going to be trained, and how they are going to be trained on how to use it. It is the maintenance, the economic impact you are going to have.

It is extremely complicated, and incentives do go a long way into helping people make that first step, because if already the cost is so completely out of whack with what they are looking at, but there is a need and they perceive a need because they would like to secure their assets, they cannot even make that first step. So it is very critical to have that piece of the pie.

Mr. SHUSTER. Mr. Orszag, do you want to comment?

Mr. ORSZAG. Sure. In terms of the causes of firms not investing adequately in homeland security, I think the main ones have already been mentioned; in particular, that the probability of an attack on any specific installation or facility is very small, and perceived to be small.

And secondly, even if it were correctly perceived, that there is what economists call a negative externality. Not all of the costs that are imposed from that attack are imposed on the firm itself, so there is no incentive to—you know, in a market-based system to protect against the spillover effects that would affect external parties.

I do want to, because I think it is so important, I do want to just emphasize. My comments on the rural malls was not to denigrate them in any way, but rather that we have limited resources. We cannot protect every single facility in the United States against attack.

We have to prioritize. There has to be some system of prioritization either from private firms doing it themselves or from the federal government or from some other source because the way to kill the economy, the way to educe unbearable economic cost for very little improvement in security is to try to protect everything. So we need some sorting of catastrophic risks versus non-catastrophic risk, and I will be blunt.

Yes, a chemical facility is more important to protect than a shopping mall that 100 people a day visit.

Mr. SHUSTER. And I think that is what is happening today is the rural malls are not investing great dollar amounts, and our chemical plants are doing those types of things.

So I will yield to the ranking member, Ms. Velazquez.

Ms. VELAZQUEZ. Thank you, Mr. Chairman. Mr. Orszag, it seems that the panel agreed that we need to invest more, but how do we get there? And we are discussing one option through tax credits. Would you please comment on other options beside tax credits?

Mr. ORSZAG. Sure. For whatever it is worth, I think the most promising approach in many settings, I talk about this some in my written statement, is a hybrid system in which you use market forces from insurance firms and third-party auditors backed up by very flexible market-based regulatory standards where necessary,

but mostly on the third-party auditor and insurance firms playing off of the collective wisdom that firms are good at doing these, including some of the firms represented here in providing security assessments and security plans with some incentive through, basically through insurance premiums.

What I would advocate—this is sort of a mix system which might be similar to what happens with a house or when you drive your car. With a house, there are a minimum building standards, building code, local building code that applies, but then in general when you go to get a mortgage the mortgage firm requires that you also have insurance. And if you put in a security system, you can get a break on your insurance premium. That provides some incentive to go beyond the minimum building code.

If one had a system of more widespread anti-terrorism insurance, that could be a dynamic market-based system of providing incentives without rigid bureaucracy, because the firms would be able to keep pace, and frankly, I think it would do a better job of keeping pace with threats and best practices than having a completely decentralized system where each individual firm sort of has to figure things out for themselves. The insurance firms working with third-party auditors could do a lot of the heavy lifting for us.

This has shown to be effective and workable in the area of safety as opposed to security at chemical facilities. Delaware and Pennsylvania, for example, have implemented a system like this on a pilot project, and it has proven to be quite effective.

Ms. VELAZQUEZ. Any—Mr. Chace.

Mr. CHACE. I would like to comment a little bit. Homeland security or terrorism insurance, as it is being called, is also very expensive. And so we are not just talking about incentives.

And I agree with the hybrid approach because I think there has to be a myriad of options. There has to be a menu that is available because one size does not fit all as we talk about security subjective.

But I think you have to be very careful about promoting overuse of insurance because that just becomes just as costly as it would to ensure a facility. So you have to balance that out.

One of the things I would recommend though as we talk about a hybrid approach here is that there are some very good instances of public/private partnerships working to define these situations and these problems at the local level, and I think that, as Tom Ridge has said before, homeland security really starts at the local level and how people are going to be taking care of their individual property, how they think about it.

One of the things we want to be very careful about, we do not want to scare the heck out of everybody.

Ms. VELAZQUEZ. But, Mr. Chace, how do we get there also? How can we get people and what role the federal government can play to raise awareness that homeland security starts at the local level?

Mr. CHACE. That is an excellent question, Congresswoman. One of the things that we have been involved with the police associa-

tions is promoting this very thing of private/public partnerships. Back in January, there was a summit hosted by COPS and IACP that talks about building public/private partnerships, and this was high on the agenda. How do we energize at the local level individuals to take a more responsive role? And that is being vetted right now, the response to that, in Justice right now of that summit.

But the long and short is there has to be awareness campaigns and dollars invested with the local AHJs to help them reach out to the private sector in those communities. Downtown partnerships work very well.

There are examples in Boston, here in D.C., in L.A., in Houston. They are very successful because they begin to maximize the resources of the private sector and play upon the long-term objectives and goals of the public sector, which have a better understanding of it. Become force multipliers and you can expedentially grow the resources of any given facility, helping the private sector to define what they should be investing in as well as helping the public sector in understanding what technologies are potentially available.

Mr. DUCEY. Yes, just adding to that, I think that is excellent, but the other thing, just going back to the rural shopping mall. I will bet you that there is a fire alarm system in that mall. I will bet you that there is a security guard in that mall. I will bet you there is theft prevention in that mall. These things, you cannot just look at the major infrastructures.

And just to get back to your question, I think the biggest problem is education. Just like nobody would go into that mall unless they were sure that there was some sort of fire system in there, we have to educate the public and educate people that they are going to know that, hey, I am not going to go work in that high rise unless it is compliant with whatever it might be.

And whether it is mandatory or not, I do not believe it, it should be mandatory, but at the end of the day if you go through what a company would go through to say I want to secure my building and I want to make it better, obviously you have to help them out with in terms of cost, but you also have to help them out in just terms of, well, what do I do to make this better, and why should I make this better, and can you help me by telling me what is my biggest threat, and that type of—by supplying that type of resource to them, I think it would help incentivize them, and then you could potentially protect every single facility in America because it—like you were just saying—it cannot just be all the public and it cannot be just all the private either. It has to be the both in combination.

Ms. VELAZQUEZ. Thank you.

Mr. Hyslop, as a firm who provides security consulting, I am sure that some of your clients are small businesses. I sense that many small businesses do not have the security measures in place that large corporations may have for different reasons, and one is cost.

Do you find that this is the case because small firms see less of a benefit from the investment, or that they simply do not have the resources to pay for the security equipment and plans?

Mr. HYSLOP. My estimation is they do not have the resources to do the work. Thinking back over the last couple of years we have talked to hundreds of organizations about security planning. Very few have actually gone forward with a plan and implementation. So it is—and when you press for the reason it is just we cannot afford to put that kind of money into this stuff because we do not see any return on that investment.

You know, small businesses are fighting the cash flow battle all the time. I mean, you talk about insurance. My professional liability insurance has gone up 100-fold since 9/11. I have to have that insurance. You know, I do a lot of work in the federal sector. It is a mandate, so I have to buy that. I do not have to buy this other stuff.

So if I have a little pot of money and I have to make a decision of what to do with it, that is how that decision gets made. If there is no incentive to do this, and as a manager you look at it and you say, well, the risk is actually pretty small, so I will take the risk.

Unfortunately, it is not just their risk as we have all said. If something bad happens, it is not just that business. So what you have basically is a business manager making a business decision that affects everybody.

Ms. VELAZQUEZ. Mr. Orszag?

Mr. ORSZAG. Yes. Could I just comment quickly? If the concern is one of firms that have sort of credit constraint cost problems, one, my understanding, and please forgive me if I misread the legislation, but the legislation is not limited to small businesses. This is a general business credit.

One approach one could take if you were particularly worried about the costs associated with small businesses is to adopt more—and coming back to the bonus depreciation versus Section 179—adopt more of the Section 179 kind of approach which is effectively limited to small businesses because it is taken back as the scale of your activities goes up, which would, if this is the concern, focus the activity or the federal tax break more on the area of concern rather than a much more expensive approach that is universal.

Ms. VELAZQUEZ. Thank you, Mr. Chairman.

Mr. SHUSTER. Thank you.

A question that I have for Mr. Ducey and Mr. Hyslop since you are out there dealing with small companies, I imagine, large, medium, large and small companies.

What type of firms are you dealing with? Because I am viewing this as a restaurant in Altoona, Pennsylvania probably does not need or have any security. I am sure they do not. But a New York restaurant 21 Club or somewhere with a lot of people come, a lot of maybe high profile targets come, they may need security and have different types of security.

What type of firms are you dealing with, the two of you? Mr. Ducey, you are in the equipment business basically?

Mr. DUCEY. Right.

Mr. SHUSTER. And Mr. Hyslop, you are dealing with the assessments, so if you could maybe—

Mr. DUCEY. From a company marketing technology, we deal with a lot of companies that have either work in high-rise buildings or in major areas.

What we deal with namely when it comes to the type of company, small businesses, and where the biggest problem is that they do not know basically what the problems are. They do not know how to address the situation. They do not know how to—what sort of problems they should be putting into place.

One of the issues is if they could be educated more, whether it be through the State Department or whether it be through the Small Business Administration, that is really what they are looking for more than anything.

Mr. SHUSTER. Mr. Hyslop?

Mr. HYSLOP. We deal with a wide variety of businesses. I can off the top of my head think of—we had a recent client that was a cryobank, freezing center, I will not go into a lot of details, but they had some unique security requirements because their customers are very sensitive about being photographed. So cameras were out. That is what I mean when you deal with culture.

So we deal with those kind of places that are sort of high-level scientific research, those kinds of things, and they are often targets of—generally when we talk about terrorists here we are all thinking Al Qaeda and that type of stuff, but we have lots of homegrown terrorists, there are eco terrorists, and there are, you know, extreme anti-abortionists people.

Mr. SHUSTER. Sure.

Mr. HYSLOP. And they are all threats, so we deal with that. Like I said before, we have dealt with water companies. All of these people are at risk. It just depends on—

Mr. SHUSTER. Right.

Mr. HYSLOP. —how you evaluate that risk.

Did that answer your question?

Mr. SHUSTER. Have either of you dealt with—rural malls came up which, again, I think is a very low-level risk out there at this point, but malls outside of—in New Jersey, for instance, have you dealt with malls and gone in to assess their—

Mr. DUCEY. Sure. I mean, we have dealt with owners of malls and other buildings and things. And when you say deal with them, what we do is—obviously we are trying to sell a product. Our product, for example, can detect—one of our products can detect illicit vapors. And we will approach a mall and say do you know what would happen if somebody walked in here with a can of mustard gas or something like that, and let it off.

Basically what it comes down to is they obviously care but at the end of the day it is either, (a) it is not going to happen here or what are the chances it is going to happen here, I have got a lot of other pressing issues; and (b) I am not even sure what to do about it. Is your product the best? Is there another product out there I should be looking at? Is this the biggest threat that I have to my mall?

Maybe I should be worried about something else, and that is basically the problems that we have had coming in, and that is where, frankly, I think the government could help us out, again, like through educating them, letting them know these solutions are available, this is the biggest threat to your mall, letting the public know that, you know, when you walk into that mall they are not taking the adequate standards necessary to really protect you much like I was saying earlier with fire or theft or something like that.

Mr. SHUSTER. That is a great concern of mine. As we harden or secure some of these high-profile targets, they are eventually going to turn into the malls and the grocery stores where they can kill 50, 60, 100 people, and that is, I think, something we are not paying attention to.

And the market, we keep talking about the market driving it. The force in the market that is going to drive this is going to be another terrorist attack.

Mr. DUCEY. Right. It will be worse than that if you think about it. Excuse me. But the perception is that I am safe as long as I am out of D.C., I am safe as long as I am not in New York, I am not next to a nuclear plant, I am not next to a chemical plant. Heaven forbid they do attack that rural mall with 100 people in it. That is obviously, as we think about, you know, maybe not a big target, that is going to threaten every single person in America and make them all feel uncomfortable, and that is obviously a huge concern.

Mr. SHUSTER. Right.

Mr. CHACE. One of the things I wanted to add, Congressman, to that is we have to take into consideration, I will give you an example.

Remember after 9/11 hit, if you had any access to the internet within the months after that, you were probably bombarded by gas masks and radiation pills, and buy this. It was crazy, and people responded basically to fear and lack of education and knowledge, and that is the worst place you can be.

We are in a position right now to plan and make some good plans for the future. That small restaurant in Altoona might not have a need for security equipment, but I bet you they have a need for understanding what they should do if the mall down the street does become a soft target hit and we do find the terrorists are not just leaning to the hard, high visibility targets, they want to strike at heartland targets, and they want to scare us.

What better place to do that then the local mall where you have basically people who are average Joes walking through with their

wives, their kids. I mean, it is a target. I do not care what you want to call it.

But the point here is we can begin to at the federal level, whether it is through incentives and tax credit, this is just, again I will say it, it is just like security, it is one component to a total solution. This is just one aspect of the discussion that needs to go on. There need to be, as we talked about earlier, a campaign to fundamentally understand and let people understanding what security requirements are, and they are not just technology issues. They are policy and education issues that you need to train people how to think about these things ahead of time so when the actual instance happens you are not playing catch-up.

Mr. DUCEY. Let me just say one thing. Think about the economic impact too to every other mall in America and every other small business.

Mr. SHUSTER. That is right, and back to an ounce of prevention or the pound of cure.

Mr. DUCEY. That is correct.

Mr. SHUSTER. Do you have another question?

Ms. VELAZQUEZ. Yes, thank you, Mr. Chairman.

Mr. Chace, your organization has numerous members that are small businesses, and obviously much of the spending on homeland security comes from the federal government, and some firms that may be clients of yours, of your members has security in place because of government requirements.

Do you find that federal agencies involved in issuing contracts as well as rules and regulations regarding security measures account for the needs of the small security firms?

Mr. CHACE. That is a good question, and I do not pretend to have that answer completely because that would require a great deal of survey work, and I do not want to mislead you.

I think that as a general rule security as we talk about here is generally misdefined and misunderstood, and misapplied most oftentimes. So some of those very agencies that might be writing regulations or specifying certain useful to these technologies have to be very careful they are not being lobbied the wrong way.

One of the things we do as an organization, and we try to educate our members so when they do this type of lobbying that they are going in and talking about what is the problem you are trying to solve. Let us understand and define the problem first because then we can plug in different types of solutions. Those might be technology. They might be policy. They might be people. They might be protocols. They might be all of the above.

But I do not think there is a fundamental understanding at the agency level about how to define this problem and get their hands around it. It is a massive issue and it is a massive problem, and we just have to make sure we are all singing from the same sheet of music, and that is a difficult task.

Ms. VELAZQUEZ. Have you come across with any particular federal agency that are most likely to ignore any of these small firms?

Mr. CHACE. Ignore the needs? I think what happens—I do not think any agency is trying to ignore anybody's needs. I think it is a resource issue. Truly trying to understand what the needs are of those small constituencies because eventually the small constituencies all add up to one big constituency if you ignore it.

Ms. VELAZQUEZ. But it is very easy for bureaucrats in Washington—

Mr. CHACE. Very easy.

Ms. VELAZQUEZ. —and I am sorry, I do not intend to sound like a Republican, I am a proud Democrat.
[Laughter.]

Ms. VELAZQUEZ. But you know, there is—and they issue rules and regulations without regard to the economic impact that—

Mr. CHACE. That is right.

Ms. VELAZQUEZ. —this might have on small businesses, but also it is not only to explain those rules and regulations for small businesses. If there is any type of outreach coming from the agencies plus—

Mr. CHACE. I would say there is minimal outreach now, and that would be one of the programs. It is a totally different discussion. I think this is again focusing on the small business aspect of this, but I think there desperately needs to be some outreach from the agencies to help.

As we talked about before, what do I do to assess my risk? How do I do that? And do I need to spend thousands and thousands of dollars just to get an assessment to find out I do not need security? I mean, that is not fair either.

So we have to make sure that the government has put out the resources, and Justice is trying to do some of this through the COPs program and some of the work that they are doing with building the public/private partnerships. They are trying to put out the models that demonstrate to small businesses and downtown partnerships how you can work together and invest the resources you have, but there needs to be a better organized effort on that.

Mr. SHUSTER. Ms. Velazquez, you do not sound like a Republican. You sound like a defender of small business.

Ms. VELAZQUEZ. You bet.

Mr. SHUSTER. You have been in this Committee for a number of years, and I appreciate that.

One last question that I have about insurance, and you can educate me on this. My understanding is that there is terrorism risk

insurance out there now in places like, you know, Madison Square Garden, for instance, I would think would have that type of insurance.

What in the insurance industry is going on as far as that goes and how is that affecting companies and facilities buying security equipment? Mr. Orszag?

Mr. ORSZAG. A couple of comments. One is—I mean, my response to the earlier question was really where I think things should be evolving towards, not what we can immediately do. My view is that the terrorism insurance market is not a particularly efficient market at this point. There are several problems in it.

One is we do have a federal reinsurance program, but there is a basic underlying problems, which is that you can be dealing with catastrophic losses here, and the insurance firms in order to be offering reasonably priced product need to be able to lay off that risk on some other entity. For really big terrorist attacks, I think the natural entity is the federal government.

I personally would have actually priced that reinsurance, in other words, charged the insurance firms for providing that service to them. That was not part of the legislation that was enacted, but that is one issue that clearly insurance firms will need some ability to lay off risk either to the federal government or to financial—the really deep, broad financial markets as a whole.

A second issue has to do with pricing that sort of actuarial process. Insurance firms did not have a lot of experience in figuring out how to price terrorism insurance, and in fact some people thought that this was something that they just could not do.

There has been significant progress, perhaps not adequate, but significant progress in developing the modeling that would be behind that. It is important to realize there are lots of things that do not happen a lot, and that are hard to predict that insurance firms do study and do provide insurance against.

So in my view, and this is a view of the Congressional Budget Office also, it is not necessarily the case that they cannot provide that kind of insurance.

And then finally, there is sort of the demand side. Even if we got an efficient market on the supply side, would this be demanded? I will reluctantly say in this context that in certain settings I think we may need to mandate anti-terrorism insurance.

The reason for that is that when you make insurance voluntary you have all sorts of selection problems that the firms that are the most vulnerable or think they are the most vulnerables are the only ones who purchase it, and it leads, just like in health insurance and annuities markets and other insurance products, it is selection effects where the market can, even if in theory would be efficient, sort of blow up, or that is not a particularly good phrasing in this context—could not operate efficiently.

So there are a variety of things that clearly need to be tackled. The market is operational but not optimal right now, and improvements are clearly warranted, but I think those improvements could be made if we focused our attention on them.

Mr. SHUSTER. I will let you go but I just want to make one comment. I would argue insurance companies have laid off that expense. As a small business owner after 9/11, my property and casualty rates went up, and my building did not burn down. You know, we did not have any problems. It was all because of what happened on 9/11.

Go ahead, Mr. Chace.

Mr. CHACE. I just wanted to make an observation. If you recall after Hurricane Andrew hit Florida, basically your insurance companies were socked with a major, major bill, and we can use that. When we are talking about catastrophic event, we can use that as a benchmark or a tool to say what will happen if we had the impact of another major terrorist attack, what would happen.

I would say, for instance, in the State of Florida instance, the insurance companies packed up and said we are not insuring anybody in Florida anymore. Sorry, you are out of luck, and we do not care. If you want insurance for this, we are not going to give it to you. So the State of Florida had to come in with some bailout on that.

I would say also that we have to be very careful about creating another impact of an event. For instance, insurance, if they are hit very hard by multiple attacks in the United States, what does that do to the insurance rates, number one? Number two, what does it do to the cash flow that they then have to begin to payout on those? And you would bankrupt almost an entire industry.

So you have to be very careful that you are not setting up one potential solution that is going to backfire on you and offer some false security in terms of that.

Mr. SHUSTER. Anyone else care to comment?

Mr. HYSLOP. Yes. I have done some work with—tried to do some work with insurance companies on offering programs to them where if you did certain things in security, their rates would go down. I have to tell you they have absolutely no interest in lowering their rates at all.

Insurance companies are about selling insurance, and I would agree that they really do not have a good way of rating a terrorist risk, so they are scared to death of selling that kind of insurance.

Right now, and I have talked to a couple of the major ones in the country, they are like they do not want to know, hands-off, call us in 10 years maybe.

Mr. SHUSTER. Anybody else care to—

Mr. DUCEY. Just going back to the question, Representative Velazquez, you had asked if the agencies are ignoring small businesses.

There is one agency out there that I think a lot of people are turning to called the Technical Support Working Group and also HSARPA that is developing new technologies. And as good as work that they are doing, they are, in my opinion, way underresourced

or way underfunded in terms of being able to look at all the different technologies.

We have gotten grants through them, and they have been very good. We have developed products and helped them and get them commercialized. They are still in the process. But at the end of the day I know there is a lot more products that we would also like to get through them as well as other companies, and frankly, they are just underresourced.

Mr. CHACE. I would like to, if I could, bolster that too because we work also with the Technical Solutions Working Group. It is the Department of Energy. It is procurement officials that get together and talk about procuring technologies for the U.S. Government. And they have reached out. We are helping to develop performance-based testing standards with them through Sandia Labs and some of the other testing agencies through DHS.

But I agree, they are severely underresourced, and any kind of activity that could put some resources into their hands would help them begin to test products so they would be products the government could procure that they know work to a certain level.

For instance, you know, if you have a camera in the middle of a desert, they are testing to see if that camera will work under those conditions. It is not a pass/fail. It is just basically environmental testing. And then GSA will help to put that on their schedule list to say this is something that has been tested, and we can pretty much rely on the testing and say it will work under the following conditions so the government is not repurchasing equipment because it did not work the first time.

So I totally support that. It is a very good activity.

Mr. DUCEY. Other agencies will rely on that to know—

Mr. CHACE. That is right.

Mr. DUCEY. —this is where we can turn to to find these technologies, to find the right products and services to help us.

Mr. CHACE. And then the incentives kick in, and then you can say that is great, so now I know that I am buying something that the government has actually tested to say it will work, and that is very helpful.

Mr. SHUSTER. Ms. Velazquez, do you have anymore questions?

Ms. VELAZQUEZ. I am not quite clear if I understand what you are saying. Small businesses that provide the type of technology for our government, and they are not getting the contracts with the government? They are not winning those contracts?

Mr. DUCEY. Well, I guess it is three different things. If I am a small business and I am trying to protect my restaurant or whatever, and for whatever reason I want to protect myself against a harmful act, the first thing is that a lot of the technologies out

there are not priced sufficiently or not developed sufficiently to be able to help that restaurant.

What HSAPRA and Technical Support Working Group are doing is basically funding companies, other small businesses who develop those products to try to get them into a form that they can then be commercialized so that then I can market it to that.

In addition to that, they are also sort of screening the products so that the small restaurant owner does not have to go through 15 different products to decide, I wonder if this one works better than that one or whatever. This way the group itself is going to say, no, this is the one that works, it is the technology. We took it from, you know, let us say the omega stage, you know, to the way that the product could be commercialized and sold to you, and therefore here is our stamp of approval, and here you go.

Ms. VELAZQUEZ. Thank you.

Mr. SHUSTER. Okay. Well, I want to take this opportunity to thank you all again for being here today, and this is a huge problem. I think that it does take a number of different—it takes the insurance industry and government, but I think this is an important part of it, putting on a tax incentive to get our businesses to look at this and invest in these assessments, and the technology to protect their businesses, and in the long run I think it does not exacerbate our financial picture. It actually helps. It becomes a multiplier effect, one of you used that term. When you have small business and business out there protecting themselves, it is, I think, less burden on the federal government that we have to spend those resources.

So again thank you all very much. I appreciate your time and your testimony, and with that the hearing is adjourned.

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

Good morning and welcome to the Subcommittee on Rural Enterprise, Agriculture and Technology. Today's hearing will focus on HR 3562, "The Prevent Act" introduced by my colleague Representative Shuster.

In today's post-911 world, businesses need to take precautions against the possibility of a terrorist attack. However, it is often times very expense to secure a business against the possibility of a terrorist attack. Business must outlay a great deal of capital to guard against a terrorist attack. Moreover what is the likelihood of a terrorist attack against a specific business? Probably pretty small.

While we are fortunate that we haven't had a terrorist attack in three years, it has also dulled our senses. But we surely know that the United States is a target. We also know that as we increase our security, Al Qaeda makes changes accordingly and they are innovative. No one can say what the next target will be.

Besides the terrible human loss we suffered on September 11th, our economy suffered terrible losses as well. We must safeguard the livelihood of people as well as their safety. HR 3562 provides an incentive to business through tax credits. I think it is one of many ideas that need to be looked in order to keep safeguard population and our economy. I now turn to Mr. Balance, the ranking member of this committee for his opening remarks.

TESTIMONY CONCERNING "TAX INCENTIVES FOR HOMELAND SECURITY RELATED EXPENSES"

Testimony of:
James E. Hyslop
President, Standing Stone Consulting, Inc.

Thank you for the opportunity to participate in this hearing.

I am the CEO of a security consulting firm based in Huntingdon, Pennsylvania. I deal with both small and large companies that are trying to improve the security of their workplace and workforce.

Small business and other small organization managers must decide how to allocate their precious resources. Often security planning and implementation is like buying insurance, a hedge against a probable event. Something bad may happen but then again it may not. When resources are scarce managers are forced to opt for placing their resources where they will provide a good return.

Most of the time this is OK, but when it isn't it usually means catastrophe for the business and frequently puts the general public in danger as well. Exploding bombs, biological agents and other threats do not discriminate in their target selection.

Our experience after hundreds of security assessments is that most organizations do not have a security strategy or plan. We see the use of security tactics that may or may not be appropriate for their intended purpose but there is no plan or understanding of how the tactics should be used. All too often the money spent on these tactics wasted.

I believe it is good policy for the government to provide financial incentives to small businesses and organizations to plan and execute a security strategy. With out such an incentive it will not get done and that puts all of us more at risk. The introduction of legislation such as the Prevent Act, sponsored by Congressman Shuster, is an important step forward towards government taking a more active role in this effort.

The assessment process is the basis of security planning. It determines where you are now and allows you to set and prioritize reasonable goals for where you want to be in the future. An assessment identifies the assets, (people, property, and processes) that need protection. It also identifies the probable threats these assets may face and how they are vulnerable to those threats. The consequence of a carried out threat is the risk the organization faces.

Once the risks are understood a plan can be developed to mitigate them. Qualified security professionals have the knowledge and experience to guide the planning process so that it will work in the culture of the business. All tactics do not work equally well in all situations. Security planners understand how tactics can and should be used to

effectively mitigate the risks. Once there is a plan and the appropriate tactics have been determined the implementation can be managed by the business owners.

The Difference between Strategy and Tactics
Our experience has been that the difference between strategy and tactics is rarely understood. Too often there are no clearly stated security goals and no way to measure if any progress is being made.

To clarify the difference between strategy and tactics, a security *strategy* is a plan to achieve the desired goals, while *tactics* are those actions taken to achieve the strategy.

Tactics are ultimately chosen to modify behaviors by deterring, detecting, delaying, or denying the ability to behave inappropriately. Strategy is determining what types of behaviors you wish to discourage (and which types you wish to encourage). During an assessment, vulnerabilities and behaviors are identified from which strategies are developed, only *then* should tactics be selected to produce the desired behaviors.

For example, Closed Circuit Television, CCTV, is a popular security tactic, but how does CCTV deter, detect, delay or deny? CCTV is basically an investigative tool. It watches and can record activity, however, it does not respond to what is seen. If the asset being protected requires an immediate response to a threat then CCTV alone is not an appropriate tactic. It must be supported with other tactics and procedures.

Equipment manufactures often offer free assessments but you always seem to need the equipment they are selling be it cameras, card readers, guard service or whatever. The equipment is installed without a clear understanding of what it can and cannot do and it often provides a false sense of safety and security. This can cause people to let their guard down by relying on technology to do things it really cannot do. The result is that you may actually be more at risk.

No security plan can be 100% effective, but being 90 or 95% effective is a great improvement over where we are now. The point is without an assessment and strategy we frequently waste money on tactics that may not deliver the expected results.

Thank you again for the opportunity to take part in this discussion.

The Security Continuum

Because of recent tragic and well-publicized events, *security* has taken on new meaning and importance. Security has become synonymous with those measures taken to protect ourselves against raging co-workers, unbalanced attackers and now, radical terrorists. This has resulted in a barrage of often intrusive tactics being touted as the answer to our security needs.

However, for a security strategy to be successful the mission and culture of the organization must be clearly understood. For example, a business is there to provide products and / or services to its customers, but each business accomplishes this mission in its own unique way. Each business has its own culture and any successful security program must understand and work within that culture. Security should not become so intrusive as to interfere with the mission of the business.

There are many stakeholders and other influences that go into determining a business's security strategy. Certainly the managers and workers have a great impact but so do customers and other members of the community such as police, fire and rescue, and government administrators (i.e. federal, state and local governments). The business's maintenance personnel are critical to any successful security plan, as is having effective training, and supportive policies and procedures. All of these things affect how a business plans and executes their security strategy.

For a security strategy to be successful, it must be understood who and what is being protected and from what kind of threats. The strategy should be a continuous process that integrates the users of the facility, the neighboring community, the appropriate tactics, outside agencies (such as police and rescue personnel), training, maintenance, and policies and procedures that support all of these components. This is what we call the *security continuum*. Without a strategy that ties all of these things together the individual components may not provide the expected benefit and may fail.

Safe, secure and responsive environments are created through assessing risks and vulnerabilities and developing a comprehensive security strategy that addresses those actual threats and perceived risks within the context of the business's mission and culture.

Strategies and tactics often get confused but the end goal is a secure environment. To clarify the difference, a security *strategy* is a plan to achieve the desired goals, while *tactics* are those actions taken to achieve the strategy.
There are three main classes of tactics:

1. ***Natural Tactics*** Are tactics that utilize the physical environment and normal every day activities to accomplish the desired result.
   Example: Designing the main entrance so that users are naturally directed and drawn towards it makes anyone attempting to gain entrance elsewhere very conspicuous. Their inappropriate behavior is immediately questioned and an appropriate response initiated.

2. ***Organized Tactics*** Are planned actions designed to improve safety, security and emergency response capabilities?
Example: A Security Officer, program utilizing organized and planned surveillance and deterrence to better protect the business and its users.

3. ***Technical Tactics*** Are mechanical tactics that aid human involvement.
Example: CCTV for visitor identification, or CCTV to aid surveillance of areas that cannot be observed by legitimate users in the normal course of their duties.

Tactics are ultimately chosen to modify behaviors by deterring, detecting, delaying, or denying the ability to behave inappropriately. Strategy is determining what types of behaviors you wish to discourage (and which types you wish to encourage). During an assessment, vulnerabilities and behaviors are identified from which strategies are developed, only *then* are tactics selected to produce the desired behaviors.

Many times tactics are chosen without a thorough understanding of the behaviors that the tactic may influence. For example, card readers and lock systems are often touted as "access control" but once a door is opened, anyone or any number of people may enter. Misapplied tactics often create a false sense of security and create potential liabilities, because they do not always produce the expected results, i.e. card readers, by themselves, cannot tell who or how many people come through a door once it is opened.

So how does an organization develop a strategy and choose tactics that will work for them? Let us consider the previous example of access control. Ask the basic question of who and what is being protected? In most facilities it is the people first, followed by the property and then protection from disruption of the mission. So if we are protecting people first, from what kinds of threats? It, of course, depends on the facility. Are the threats internal or external? Is the user population known and easily identifiable or is it transient? What types of inappropriate behaviors can be expected? Obviously the strategy must be tailored to the specific circumstances – **in security one size does not fit all.**

When tactics do not fit into a comprehensive strategy and *people* are not at the core of that strategy, the tactics will inevitably fail. The best lock in the world is of little value if doors are propped open. If the security planner knows the door will likely be propped open (the culture is understood) then another more appropriate tactic can be selected to protect unauthorized entry through that particular door.

Each school must develop its own strategy and its own unique set of tactics. Understanding the interrelationships of the *security continuum* and using them appropriately to improve security is the key to having a safe and secure school.

TESTIMONY OF

KEN DUCEY

PRESIDENT

MARKLAND TECHNOLOGIES

FOR

SUBCOMMITTEE ON RURAL ENTERPRISES, ALGRICULTURE, AND TECHNOLOGY

OF THE

COMMITTEE ON SMALL BUSINESS

U.S. HOUSE OF REPRESENATIVES

AT IT'S HEARING ON

TAX INCENTIVES FOR HOMELAND SECURITY RELATED EXPENSES

July 4, 2004

TESTIMONY OF KEN DUCEY, MARKLAND TECHNOLOGIES, FOR HSIA

Mr. Chairman, members of the Subcommittee, is a pleasure to appear before you today. Accompanying me today is Bruce deGrazia; Chairman of Homeland Security Industries Association (HSIA) was organized in November 2001, and formally launched over a year ago. We have over 400 members, ranging from multi-billion dollar defense contractors, to mid-sized firms to start-ups and incubator firms. Our panel today reflects this cross section.

In my oral presentation today, I will summarize the views and recommendations of HSIA. We ask that our complete written statement, which will be filed separately, be included in the record of this proceeding. The Association's views represent the consensus of HSIA members but not the particular views of any one member. In general, HSIA strongly supports legislation such as HR 3562 to provide tax incentives to promote private sector Homeland Security initiatives.

TESTIMONY OF KEN DUCEY, MARKLAND TECHNOLOGIES, FOR HSIA

DISCUSSION

Since 9/11, America has begun a fundamental transformation from an open society to one that must continually weigh the security of its citizens and corporate assets from terrorist attack. In the immediate aftermath of 9/11, the Administration and the Congress acted with vigor. Unfortunately, partisan politics in the Legislative Branch held up rapid increases in HLS funding, as that Congress did not release FY 2003 funding until nearly half way through the current fiscal year. This meant that the substantial increases in HLS funding that had been anticipated last fall - for First Responders and others - did not begin to be released until 17 months ago. Since then, the Administration has moved quickly but First Responders and others involved in HLS still have many needs, for which funding has just begun. As a consequence, it is understandable that frustrations have been felt among First Responders throughout the country and among the companies who hope to serve them, including HSIA members.

America is an open society. That is the strength of our democracy and the source of our vulnerability. Two years ago, on the first anniversary of 9/11, the Washington Post analyzed America's vulnerability to terrorist attack and gave us an overall grade of "C-" for HLS. Of course, this is unacceptable. America faces a challenge, which is likely to take years to accomplish. Therefore, we repeat a call we made in Congressional Staff briefings in January and February 2003 for an end to partisanship in HLS.

TESTIMONY OF KEN DUCEY, MARKLAND TECHNOLOGIES, FOR HSIA

Our concerns about the HLS fall into three categories: (a) federal procurement; (b) state and local procurement and (c) private sector initiatives.

With respect to federal HLS procurement by DHS and other federal agencies with related procurements, we believe that the Administration has done a commendable job in successfully launching the new Department in a very short time, as well as in meeting its deadline to federalize airport passenger and baggage screening. In addition, we commend the Department for its so-called "Industry Days". DHS has gone to great and commendable lengths to outreach to the federal contracting community to share with firms DHS's vision, acquisition plans and updates about its programs.

However, we have communicated to Congress on other hearings constructive suggestions to help improve this system in the future. We believe that the incidence of sole-source contracts, and sole-source delivery orders off the GSA Schedule, should decrease.

Today we address the need for tax incentives for Homeland Security related expenses. In the April 6, 2003 Sunday New York Times, an article appeared which predicted that by 2008, annual HLS spending would increase from he 2003 annual level of about $60 million to $200 billion annually. And the article predicted that 2/3 of this

spending would be in the private sector. Yet the bet estimates we have seen suggest that since 9/11, private sector spending for HLS has increased only 4%. HSIA worked with a group organized by the American National Standard Institution (ANSI) from January 2004 to May 2004. The purpose of this group was to develop a recommendation for the 9/11 commission to help promote development of voluntary private sector HLS standards. We accomplished this and made a recommendation that NFPA 1600 serve as a model or framework for HLS private sector standards.

This led to a discussion about how to induce the private sector to invest in HLS measures and equipment. This is a critical issue since the vast majority of U.S. critical in the structure is privately owned. The consensus of our group, which included over 40 organizations, was that the 9/11 commission should recommend to Congress tax incentives. Not only for private companies investing in HLS initiatives, but also for municipalities.

In conclusion, we strongly support the committee's efforts on this important subject. We would be happy to answer any questions. Thank you.

Ken Ducey

Testimony of Mr. Richard Chace, Executive Director of the Security Industry Association (SIA)

Chairman Graves, Ranking Member Ballance, other members of the Subcommittee, thank you for giving me the opportunity to participate in this important hearing on tax incentives for homeland security related expenses and in particular H.R. 3562, "The Prevent Act" that was introduced by Congressman Bill Shuster.

My name is Richard Chace and I am the Executive Director of the Security Industry Association. It is my honor to testify today on behalf of the Security Industry Association (SIA), which represents over 700 electronic security equipment manufacturers, distributors, and service provider organizations around the country and throughout the world.

For more than 35 years, the Security Industry Association (SIA), a non-profit international trade association has represented electronic and physical security product manufacturers, specifiers, and service providers.

As an association our primary mission is to promote growth, expansion, and professionalism within the security industry by providing education, research, technical standards, representation and defense of its members' interests.

The member companies of our association employ roughly 150,000+ individuals. Yet while this is a sizable constituency, and fraction of the industry as a whole, the majority of our members employ rough 500 employees or less. This, according to the U.S. Small Business Administration, is the definition of a small business and it is indicative of the significant number of security industry companies and employees that are affected by small business laws and regulations.

It is because of our industries vulnerability to the affects of small business laws and regulations that the Security Industry Association is in strong support of H.R. 3562, "The Prevent Act" as introduced by Congressman Shuster. We applaud Congressman Shuster's leadership in introducing this critical piece of legislation. We would also recognize Congressmen Weller and Crowley for their collective work and focus in this area in past sessions.

Given the increased focus on the private sector's role in homeland security and the many economic benefits that can arise from appropriate security applications, it is vital that private sector businesses are given the tools needed to properly secure employees, customers and important assets.

Passage of Congressman Shuster's legislation H.R. 3562 would be a major step in promoting the private sector's role in meeting the post-September 11th challenge of adequately securing the homeland. This important bill provides appropriate tax incentives for businesses to enhance their security while simultaneously promoting safety for employees and customers and enhancing productivity.

In today's uncertain world, the private sector and the government need to work together to provide a more secure environment for places such as malls, movie theaters, stadiums, hotels, apartment complexes and other public areas. H.R. 3562 would provide the necessary incentive for businesses to apply state of the art security technology to protect our local restaurants, businesses, and other soft targets.

Last year, Congress passed and President Bush signed into the law the Jobs and Growth Tax Reconciliation Relief Act of 2003 (H.R.2) which allowed for an increased amount (up to $100,000) for tax expenses, as well as an increase in the bonus depreciation from 30 – 50%. This increase allows especially small businesses the opportunity to upgrade or purchase security systems.

This in turn helps sell these products and help more than half of our membership. These tax breaks are a win-win situation for the customer and the manufacturer.

This legislation runs out as of January 1, 2005 and the ability to take advantage of securing small businesses and their assets will be lost. These provisions act as cost-effective tools that will help America's businesses play an increased role as a force multiplier in homeland security. As continuing concerns over security issues place economic strains on consumers and businesses, a reliable security infrastructure has become essential to keeping businesses vibrant.

In a GAO report released on Friday entitled "Status of Key Recommendations GAO Has Made to DHS and Its Legacy Agencies" it

calls for actions to be taken by the Department of Homeland Security. In the National Strategy for Homeland Security released by the Administration in July of 2002, one of the recommendations was to determine the need for security regulations, grants or incentives for securing critical infrastructure. This has not been done, and legislation such as H.R. 3562 could play a critical role in successfully reaching this goal.

To help support the Department of Homeland Security's regulation and recommendation development, standards development should not be overlooked. In recent years, Congress has passed several laws making it clear that federal agencies rely upon private voluntary standards whenever feasible. In early 1996, the **National Technology Transfer and Advancement Act (Public Law 104-113)**, was signed into law and contained key provisions pertaining to standards and conformity assessment. Namely, that all federal agencies and departments shall use technical standards that are developed or adopted by voluntary consensus standards bodies, using such technical standards as a means to carry out policy objectives or activities determined by the agencies and departments.

Other laws and policies that reinforce the strong public-private partnership approach to standards and conformity assessment in specific sectors or areas of interest include **The Consumer Product Safety Act** (amended in 1981) and **Milspec Reform** (in 1994). Under the Consumer Product Safety Act, the Consumer Product Safety Commission is specifically to rely upon voluntary consensus consumer product safety standards rather than promulgate its own standards.

The government is a stakeholder in the development of standards, however the setting of standards should be left to the private sector. SIA supports a standards activity that is open, fair and nondiscriminatory. But more importantly, these standards should be driven by marketplace considerations, such as the need to bring products to market or meet customer demands as specified in H.R. 3562.

Government should be a participant in the standards setting process or take a role in areas that are aimed at protecting the public interest or laying the ground rules for a competitive market. Government should advocate the greater use of voluntary consensus standards and should support that by broader participation by agency personnel in standards development. This

aids the government in tackling its mandate to ensure public safety and health.

SIA supports a Standards development effort, which is beneficial to the small business end user. In the case of procurement and internal operations, 'end user' is the role that the government takes. As 'users', the government has the opportunity through standards to resolve technical problems to make security products work together, ensure lack of confusion in the marketplace and ensure the interoperability of products.

Security systems and security technology applications, when utilized in the context of clearly defined policies, provide a wide range of benefits, especially to the corporate bottom line. Sophisticated and well-planned security applications in a corporate setting provide a significant return on investment.

They play a role in the activity of the business and should not be seen as an expense or drain. Here's a list that provides just a few.

Security Productivity Top Ten List

1. Security systems provide enhanced protection against external theft and loss, which can be devastating financially to business and emotionally to workforce.
2. Security provides avenues to reduce employee theft and corporate shrinkage, which can be economically devastating.
3. Security allows for lower insurance premiums because businesses have taken steps to minimize risk and loss.
4. Security enhances safety and also provides automated tools for human resources such as time and attendance.
5. Security technologies provide data and images for measuring effectiveness of business activities such as production and marketing.
6. Security provides for dramatically increased efficiencies in managing inventory flow and control.
7. Security provides flexibility to get real time and remote status of business operations, even on a global scale.
8. Security technologies provide efficiencies that allow for easy integration of physical access control and logical database access.
9. Security can provide a greater comfort level for employees, who gain productivity and a sense of loyalty to the company.
10. Security can provide a greater feeling of comfort for customers.

In conclusion, I would like to once again thank this Subcommittee for holding this hearing. It is my hope that this initial conversation will spark greater interest in H.R. 3562 and serve as a springboard for Congress to enact this legislation. As the Executive Director of SIA, I would like to offer up my association and its members as a resource for this Committee and the Congress as you grapple with these difficult homeland security related issues.

Chairman Graves, thank you again for your attention to this matter and I will be happy to answer any questions that you or your colleagues on the Subcommittee may have for me.

Homeland Security:
The Problems with Providing Tax Incentives to Private Firms

Peter R. Orszag[1]
Joseph A. Pechman Senior Fellow in Economic Studies

Testimony before the House Committee on Small Business
Subcommittee on Rural Enterprise, Agriculture and Technology

July 21, 2004

Thank you for inviting me to testify this morning.

In homeland security, private markets do not automatically produce the best result. To be sure, private firms have some incentive to avoid the direct financial losses associated with a terrorist attack on their facilities or operations. In general, however, that incentive is not compelling enough to encourage the appropriate level of security.

Providing a tax subsidy to private firms for homeland security costs would represent one way of changing the incentives facing firms. This approach, however, does not represent sound policy, especially in light of the nation's massive long-term fiscal gap. A mixed system of minimum regulatory standards, insurance, and third-party inspections would better harness the power of private markets to invest in homeland security in a cost-effective manner.

Modifying incentives for the private sector to invest in homeland security

In other testimony and in a co-authored Brookings volume, I have presented the reasons that private firms have inadequate incentives to invest in homeland security.[2] The need for some sort of government intervention to alter the incentives facing private firms does not, however, determine how or in which situations the government should intervene. For example, to bolster safety in commercial buildings, the government could:

---

[1] The views expressed here do not necessarily represent those of the staff, officers, or board of the Brookings Institution. I thank Michael O'Hanlon, Ivo Daalder, I.M. Destler, David Gunter, Robert Litan, and Jim Steinberg for the joint work upon which this testimony draws, Emil Apostolov for excellent research assistance, and Howard Kunreuther, Janusz Ordover, and Bobby Willig for helpful discussions. For related details, see *Protecting the American Homeland: One Year On* (Brookings Institution Press: 2003).

[2] See *Protecting the American Homeland: One Year On* (Brookings Institution Press: 2003), Peter R. Orszag, "Critical Infrastructure Protection and the Private Sector: The Crucial Role of Incentives," Testimony before the House Select Committee on Homeland Security, Subcommittee on Cybersecurity, Science, and Research & Development and the Subcommittee on Infrastructure and Border Security, September 4, 2003; and Peter R. Orszag, "Homeland Security and the Private Sector," Testimony before the National Commission on Terrorist Attacks Upon the United States, November 19, 2003.

- Impose direct regulation: The Federal government could require that certain anti-terrorist features be included in any commercial or public building.[3]

- Require insurance: The Federal government could require every commercial or public building to carry insurance against terrorism, much as state governments now typically require motorists to carry some form of auto liability insurance.[4] The logic of such a requirement is that insurance companies would then provide incentives for buildings to be safer.

- Provide a tax credit for anti-terrorism measures: The Federal government could provide a tax credit for investing in anti-terrorism building features or for other steps to protect buildings against attacks. This is basically the approach undertaken in legislation proposed by Representative Shuster.

- Create a new program on the outlay side of the budget: The Federal government could directly purchase specific types of equipment for private-sector buildings.

Each of these approaches typically entails a different level of aggregate costs, and also a different distribution of those costs across sectors and individuals.[5]

Tax credits

Representative Shuster's legislation (H.R. 3562) would provide a business tax credit for various security expenditures by private firms, including for:

- An electronic access control device or system.
- Biometric identification or verification device or system.
- Closed-circuit television or other surveillance and security cameras and equipment

[3] Although building codes traditionally fall within the jurisdiction of local governments, the Americans with Disabilities Act (ADA) mandated changes in buildings. A precedent therefore exists for Federal preemption of local building codes. It should be noted that the ADA does not directly affect existing building codes. But the legislation requires changes in building access and permits the Attorney General to certify that a State law, local building code, or similar ordinance "meets or exceeds the minimum accessibility requirements" for public accommodations and commercial facilities under the ADA. Such certification is considered "rebuttable evidence" that the state law or local ordinance meets or exceeds the minimum requirements of the ADA.

[4] The McCarren-Ferguson Act delegates insurance regulation to the states. The Federal government could nonetheless effectively impose an insurance mandate either by providing strong incentives to the states to adopt such a mandate, or perhaps by mandating that all commercial loans from a federally related financial institution require the borrower to hold such insurance.

[5] In theory, the different approaches to implementing a security measure could be separated from how the costs of the measure were financed – for example, firms adhering to regulatory standards could be reimbursed by the Federal budget for their costs. In practice, however, the method of implementation often implies a method of financing: the cost of regulations will be borne by the producers and users of a service, and the cost of a general subsidy will be borne by taxpayers as a whole. In evaluating different implementation strategies, financing implications must therefore be taken into account.

- Locks for doors and windows, including tumbler, key, and numerical or other coded devices
- Computers and software used to combat cyberterrorism
- Electronic alarm systems to provide detection notification and off-premises transmission of an unauthorized entry, attack, or fire
- An electronic device capable of tracking or verifying the presence of assets
- High efficiency air filtering systems
- Mechanical and non-mechanical vehicle arresting barricades
- Metal detectors
- Signal repeating devices for emergency response personnel wireless communication systems
- Components, wiring, system displays, terminals, auxiliary power supplies, computer systems, software, networking infrastructure and other equipment necessary or incidental to the operation of any item described in any of the preceding subparagraphs.

This type of approach could help to strengthen firm's incentives to protect themselves against attack, but tax credits also carry several dangers:

- First, they can encourage unnecessarily expensive investments in security measures (or "gold plating"). The problem is particularly severe in the case of investments that provide protection against terrorist attack but also have substantial other benefits to firms. Consider, for example, the mundane case of door locks. Such systems can provide some protection against terrorist attack, but that is not likely to be their primary function. Yet even if the homeland security protection provided is relatively modest, though, the firm may find it worthwhile to purchase an expensive door security system if offered a 20 or 30 percent tax credit for that expenditure, since so much of the cost is borne by others. The door locks may provide significant other benefits to the firm (such as reduced theft and vandalism).

- Second, tax credits could provide benefits to firms that would have undertaken the investments even in the absence of the tax subsidy – raising the budget cost without providing any additional security. In other words, the proposed tax credits "buy out the base" of what firms are already doing to protect themselves against terrorist attack. A tax credit focused on marginal investments, albeit difficult to design and implement, would be better targeted.

- Third, tax credits do a poor job of differentiating between high-risk and lower-risk sectors, yet the degree of government intervention should clearly vary by circumstance. For example, consider the difference between security at a mall and security at a chemical facility. Poor security at a mall does not endanger remote areas in the nation to nearly the same degree as poor security at a chemical facility. The products of chemical plants could be used as *inputs* in a terrorist attack, and therefore the facilities warrant more aggressive government intervention than shopping malls. Yet the tax credits would provide the same benefit to shopping malls as chemical plants.

- Fourth, these types of tax credits unduly complicate the tax code, which is already excessively complex. Defining and implementing the specific expenditures that would qualify for the proposed tax credit is administratively complex. For example, how exactly should the IRS differentiate a computer "used to combat cyberterrorism" from any other computer?

- Fifth, tax credits would further worsen an already bleak fiscal outlook. The nation's long-term fiscal gap amounts to between 7 and 10 percent of GDP.[6] New tax credits that are not offset by other policy changes would exacerbate this gap.

- Finally, tax credits spread the cost of homeland security spending in a particular sector across the entire population, rather than the stakeholders (the owners of businesses, the workers, and consumers of the product) in that sector itself. If particular sectors are more dangerous than others, we as a society may want to discourage activity in that sector – which would be better accomplished by having stakeholders in that sector bear the full cost of protection. This cost-sharing issue is explored in the next section.

Who bears the cost?

A fundamental question in evaluating different approaches to homeland security costs in the private sector is how those costs should be shared. Tax credits at least partially spread those costs across the public as a whole; other approaches do not spread the cost in this way.

As one example, consider the higher risks of terrorism for "iconic" structures. Any additional costs of protection -- say, installing a finer filter on the air intake system to protect against bio-attack -- would either reduce the market values of such buildings or be passed along in higher rents to occupants.[7] From one perspective, this outcome seems unfair: it effectively imposes higher costs on the owners or occupants of a specific building to address a threat related to the nation's security. A tax credit for homeland security investments could instead distribute the burden across the broader tax-paying public. A tax-credit approach, however, would mean the population as a whole was effectively providing a subsidy to the owners of prominent buildings – an outcome that itself may seem unfair.

Rather than wading into this philosophical debate over fairness, I'd like to emphasize instead the role of incentives. Imposing the cost on the stakeholders rather than the general public could raise the costs of occupying the skyscrapers and therefore discourage people from living and working there. Given the buildings' assumed attractiveness to terrorists, this may be an appropriate response to diminish the nation's exposure to catastrophic attack. Basically, such

---

[6] Alan J. Auerbach, William G. Gale, and Peter R. Orszag, "Sources of the Long-Term Fiscal Gap," *Tax Notes*, May 24, 2004.

[7] For *existing* buildings, the cost is more likely to be borne by the owners of the building. For *new* buildings, the cost is more likely to be shifted forward to occupants.

a "stakeholder pays" approach ensures that those who engage in the most dangerous activities (in terms of their exposure to terrorist attacks) pay for the costs associated with those risks.

In other words, from an incentive perspective, spreading the cost of protection across the entire population would seem less desirable than concentrating the cost on the users or producers of a specific service. This perspective only augments the other shortcomings associated with tax credits identified above, leading to my view that such tax credits do not represent sound policy.

Toward a mixed system

If tax credits are not the answer, what is? All of the various approaches to government intervention have shortcomings, and the relative importance of these drawbacks is likely to vary from sector to sector. Nonetheless, in many cases that require government intervention, one longer-term approach appears to be the least undesirable and most cost-effective: a combination of regulatory standards, insurance requirements, and third-party inspections.

A mixed regulatory-insurance system is already applied in many other areas, such as owning a home or driving a car. Local building codes specify minimum standards that homes must meet. But mortgages generally require that homes also carry home insurance, and insurance companies provide incentives for improvements beyond the building code level – for example, by providing a reduction in the premiums they charge if the homeowner installs a security system. Similarly, governments specify minimum standards that drivers must meet in order to operate a motor vehicle. But they also require drivers to carry liability insurance for accidents arising out of the operation of their vehicles. Meanwhile, insurance companies provide incentives for safer driving by charging higher premiums to those with poorer driving records.[8]

A mixed system of minimum standards coupled with an insurance mandate not only can encourage actors to act safely, but also can provide incentives for innovation to reduce the costs of achieving any given level of safety.[9] The presence of minimum regulatory standards also helps to attenuate the moral hazard effect from insurance, and can provide guidance to courts in determining negligence under the liability laws.[10]

---

[8] To be sure, crucial differences exist between the terrorist case and these other examples. For example, stable actuarial data exist for home and auto accidents, but not for terrorist attacks. Nonetheless, it may be possible for insurers to distinguish risks of loss based on differences in damage exposures, given a terrorist incident. Some financial firms are already trying to devise basic frameworks for evaluating such risks. See, for example, Moody's Investors Service, "Moody's Approach to Terrorism Insurance for U.S. Commercial Real Estate," March 1, 2002.

[9] Moreover, an insurance *requirement* (as opposed to an insurance option) avoids the adverse selection problem that can occur in voluntary insurance settings. In particular, if anti-terrorism insurance were not mandatory, firms with the most severe terrorism exposure would be the most likely to demand insurance against terrorist acts. The insurance companies, which may have less information about the exposure to terrorism than the firms themselves, may therefore be hesitant to offer insurance against terrorist attacks, since the worst risks would disproportionately want such insurance. The outcome could be either that the insurance companies do not offer the insurance, or that they charge such a high price for it that many firms (with lower exposure to terrorism but nonetheless some need to purchase insurance against it) find it unattractive. This preference for mandatory insurance assumes no constraints or imperfections on the supply side of the insurance market.

A mixed system also has the advantage of being flexible, a key virtue in an arena where new threats will be "discovered" on an ongoing basis. In situations in which insurance firms are particularly unlikely to provide proper incentives to the private sector for efficient risk reduction (for example, because insurers lack experience in these areas), regulation can play a larger role.

Third-party inspections can be coupled with insurance protection to encourage companies to reduce the risk of accidents and disasters. Under such schemes, insurance corporations would hire third-party inspectors to evaluate the safety and security of plants seeking insurance cover. Passing the inspection would indicate to the community and government that a firm complies with safety and security regulations. The firm would also benefit from reduced insurance premiums, since the insurer would have more confidence in the safety and security of the firm.

This system takes advantage of two potent market mechanisms to make firms safer, while freeing government resources to focus on the largest risks. Insurance firms have a strong incentive to make sure that the inspections are rigorous and that the inspected firms are safe, since they bear the costs of an accident or terrorist attack. Private sector inspections also reduce the number of audits the regulatory agency itself must undertake, allowing the government to focus its resources more effectively on those companies that it perceives to pose the highest risks. The more firms decide to take advantage of private third-party inspections, the greater the chances that high-risk firms will be audited by the regulatory agency.

Studies have shown how such a program could be implemented in practice. In Delaware and Pennsylvania, the State Departments of Environmental Protection have worked closely with the insurance industry and chemical plants to test this approach for chemical facility safety.[11]

Applying the mixed system

Three examples of homeland security issues seem relatively well-suited to a mixed system of regulatory standards, anti-terrorism insurance, and third-party inspections:

- Security at chemical and biological plants. Such plants contain materials that could be used as part of a catastrophic terrorist attack, and should therefore be subjected to more stringent security requirements than other commercial facilities. The regulatory standards could be supplemented by an insurance requirement, which would then allow insurance firms to provide incentives for more innovative security measures.

---

[10] For a discussion of the potential benefits of a mixed system of building code regulations and mandatory catastrophic risk insurance in the context of natural disasters, see Peter Diamond, "Comment on Catastrophic Risk Management," in Kenneth Froot, ed., *The Financing of Catastrophe Risk* (University of Chicago Press: Chicago, 1999), pages 85-88.

[11] For further information, see Howard Kunreuther, Patrick McNulty, and Yong Kang, "Improving Environmental Safety Through Third Party Inspection," *Risk Analysis*. 22: 309-18, 2002.

- Building security for large buildings or arenas. The Federal government could supplement existing building codes for large commercial buildings with minimum performance-based anti-terrorism standards. Those regulations could then be supplemented by requiring the owners of buildings to obtain anti-terrorism insurance covering some multiple of the value of their property. Adjustments to the basic premium could encourage building improvements that reduce the probability or severity of an attack (such as protecting the air intake system or reinforcing the building structure).

- Cyber-security. Since the steps involved in protecting a computer system against terrorist attack are similar to those involved in protecting it against more conventional hacking, the case for Federal financing is relatively weak. Federal subsidies of anti-terrorism cyber-security measures at private firms would likely induce excessive "investment," since the firms would not bear the full costs but would capture many of the benefits (through improved security against hacking attempts). Nonetheless, a successful terrorist cyber-attack could cripple the nation's infrastructure, at least temporarily. Some performance-oriented regulatory steps may therefore be warranted. For example, the government could require critical computer systems to be able to withstand mock cyber-attacks, with the nature of the cyber-attack varying from firm to firm. Given the ease with which mock attacks and tests could be conducted -- which could provide a basis for pricing the insurance -- an insurance requirement may be feasible and beneficial. One could even imagine insurance firms hiring cyber-experts to advise insured firms on how to reduce their exposure to cyber-attacks. To be consistent with reasonable thresholds for government intervention, any regulatory or insurance requirements could be imposed only on larger firms or those that have direct access to critical computer infrastructure components.

Conclusion

I am pleased that policy-makers are considering various ways of changing the incentives facing private firms to invest in homeland security protections. One of the most significant policy-making failures over the past several years has been inadequate attention to this problem.

Unfortunately, though, tax credits are not the right approach to altering private incentives. In addition to encouraging gold-plating, tax credits spread the cost of protecting private firms across the population as a whole. In my view, the costs should instead be imposed on the users and providers of a particular service, which ensures that those who engage in the most dangerous activities (in terms of homeland security risks) pay for the costs associated with those risks. Furthermore, tax credits would worsen an already bleak fiscal outlook.

Instead of providing tax credits, a mixed system of minimum standards, insurance, and third-party inspections could better harness market forces to provide homeland security at minimum cost. This approach can and should be supplemented or replaced when there is evidence that other approaches would be more efficient or when there are significant externalities associated with a given type of terrorism. For example, in some cases, the insurance requirement may not be necessary because lenders already require terrorism insurance to be carried before extending loans – and a government mandate is thus effectively superfluous.

Furthermore, it will undoubtedly take time for the insurance industry to develop appropriate ways of pricing policies covering potentially catastrophic attacks.

A critical challenge is deciding how extensive government regulation should be. It is one thing to set standards for commercial facilities such as chemical and biological plants. But should the government attempt to provide anti-terrorism regulations for *all* commercial buildings? For hospitals? For universities? Where does the regulatory process stop? One answer to this question is provided in *Protecting the American Homeland*, which focuses on reducing the risk of large-scale terrorist attacks.

○