THE IMPACT OF FOREIGN OWNERSHIP AND FOREIGN INVESTMENT ON THE SECURITY OF OUR NATION'S CRITICAL INFRASTRUCTURE

HEARING

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

MAY 16, 2007

Serial No. 110–36

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE
48–911 PDF WASHINGTON : 2009

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California,
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
AL GREEN, Texas
ED PERLMUTTER, Colorado
VACANCY

PETER T. KING, New York
LAMAR SMITH, Texas
CHRISTOPHER SHAYS, Connecticut
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
BOBBY JINDAL, Louisiana
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
MARSHA BLACKBURN, Tennessee
GUS M. BILIRAKIS, Florida
DAVID DAVIS, Tennessee

JESSICA HERRERA-FLANIGAN, *Staff Director & General Counsel*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

SHEILA JACKSON LEE, Texas, *Chairwoman*

EDWARD J. MARKEY, Massachusetts
PETER A. DEFAZIO, Oregon
ELEANOR HOLMES NORTON, District of Columbia
YVETTE D. CLARKE, New York
ED PERLMUTTER, Colorado
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

DANIEL E. LUNGREN, California
GINNY BROWN-WAITE, Florida
MARSHA BLACKBURN, Tennessee
GUS M. BILIRAKIS, Florida
PETER T. KING, New York *(Ex Officio)*

MATHEW WASHINGTON, *Director*
ERIN DASTE, *Counsel*
NATALIE NIXON, *Deputy Chief Clerk*
COLEY O'BRIEN, *Senior Counsel*

CONTENTS

THE IMPACT OF FOREIGN OWNERSHIP AND FOREIGN INVESTMENT ON THE SECURITY OF OUR NATION'S CRITICAL INFRASTRUCTURE

Wednesday, May 16, 2007

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON TRANSPORTATION SECURITY AND
INFRASTRUCTURE PROTECTION,
Washington, DC.

The subcommittee met, pursuant to call, at 2:50 p.m., in Room 1539, Longworth House Office Building, Hon. Sheila Jackson Lee [chairwoman of the subcommittee] presiding.

Present: Representatives Jackson Lee, DeFazio, Clarke, and Lungren.

Ms. JACKSON LEE. Good afternoon. Let me first of all thank all of the witnesses for their patience. There is quite a bit of activity on the floor of the House, and Members must be engaged in that activity. Our ranking member is en route.

Let me acknowledge the presence of Mr. DeFazio of Oregon. I thank him, and members are coming, but with the importance of this hearing and the presence of the witnesses, we will begin.

Let me first of all ask the subcommittee to come to order.

The subcommittee is meeting today to receive testimony on the impact of foreign ownership and foreign investment on our Nation's critical infrastructure.

Under the rules of the House of Representatives and the rules of the committee, visitors and guests are not permitted to make undue noise or to applaud or in any way show their pleasure or displeasure as to the actions of the Members of the House. The Chair will continue to abide by those rules as we proceed in this hearing so that all of the witnesses may be heard, as well as the members of the committee.

Let me begin with my opening statement, I yield myself 5 minutes.

I would like to take this opportunity, as I said earlier, to thank all of you for joining with us this afternoon so that we can continue to address the questions of security and the security of our Nation. In this hearing, we will continue our exploration of foreign ownership and investment and how it intersects with national security.

As we all know, early this year, this subcommittee took a thorough look into how the Federal Government monitors and evaluates foreign ownership of our critical infrastructure. Today, the subcommittee is taking a different approach to this issue.

I think it is important to note that the challenge of the Department of Homeland Security and the challenge, of this committee is to be proactive. It is important that we imagine the possible and the impossible; and what that means is that every hearing that may in some areas be viewed as impossible are the actions that would generate from the testimony or the suggestion of the title to be impossible. We who have the responsibility of securing America can never consider that the possible or the impossible is too small or too narrow for us to review.

Today, we are exploring the vulnerabilities of critical infrastructure owned by U.S. companies that have a significant number of foreign investors and how it may compromise homeland security preparedness, as well as the question of investment and access and control. I think we all understand that when a foreign entity establishes a lasting financial interest in a country, it is able to exert influence on that country.

According to 2005 CEA data, foreign investors own over 9 trillion in stock in U.S. assets. These assets are composed of four basic types and the largest portion is foreign direct investment. This type of investment goes directly into companies and infrastructures. The other three types of foreign investment are corporate stocks, private bonds and the U.S. Treasury bonds and bills. Each of these types comprises about 2 trillion of the total investment stocks. It is also important to note that these investments have accumulated over decades, even centuries.

Like most Americans, I wholeheartedly support capitalism and free trade, of course, with various requirements that would help all Americans. Yet, as events have shown, we need to pursue a vigorous oversight agenda, especially in the area of foreign investment and critical infrastructure. Dubai Ports taught us that we need to not just focus on one area of infrastructure, but we need to focus on all areas. And we need to be open minded because we know the capitalistic system is enormously creative. There are any number of subsets of what can be sold and what can be invested in.

As the chairwoman of this subcommittee which bears the term "infrastructure protection" in its title, I intend to do just that, evaluate how infrastructure is being protected to ensure it is here and available when America needs it most in a time of crisis.

As we all know, terrorists do not signal or call ahead before they attack. We saw this in Madrid and London, amongst other horrible incidents. Terrorists are creative, especially in the ways in which they will attack us.

It is not inconceivable that a terrorist might try to attack us not with brute force, but simply by pressing a computer button or by crippling a key asset or some other nonstated, but possibly unimaginable-type act.

Another example, foreign investment deals with energy. Current European wind companies have been keen on investing in the U.S. market. In fact, several of the largest turbine producers are now selling to U.S. developers for projects, and opening offices and manufacturing plants in the U.S.

Now, I know many will say that it is just wind turbines. What is the big deal? Well, being from Houston, I can tell you that energy is an important issue, and the security of energy is important.

We must make sure that these companies take the necessary steps to protect new infrastructure as it becomes more prevalent.

Today, we will address these basic questions. What are the U.S. companies doing to control access to sensitive information that if compromised, could possibly cripple our economy? What steps are taken to protect information when U.S. corporations operate outside the U.S.? For example, Halliburton recently set up operations in Dubai. This committee is eager to know how sensitive material or information that is housed in those offices in a foreign land are to be protected.

I and other members of this subcommittee certainly are, hopefully, perceived as being responsible and serious and seriously committed to protecting the critical infrastructure and understanding how the private sector is protecting our vital assets.

The chairman of the full committee and the ranking member of the full committee have had one voice on the question of ensuring the security of this Nation. As I work with my ranking member, we hope that as we work through many issues, that voice will be one voice on the questions of securing the Nation.

Again, today, we want to explore what steps the private sector has taken to protect its infrastructure, and I look forward to witnesses' testimony learning how these different entities protect themselves from threats and what role Congress can play to fortify and protect the United States' assets.

Let me close by simply saying that, in addition to the witnesses who are here, we know that many States have found in the public sector a source of revenue by utilizing public entities for investment of foreign operators, investors, and sometimes owners. In the course of our work, we will be looking at those issues as well, because frankly, the ability to lose control during a time of crisis or tragedy has to be the concern of this committee.

So, in the course of this hearing, I will put some of these thoughts into the comments and questions that I will make. We must stand ready and we must be prepared.

The Chair now recognizes the ranking member of the subcommittee, the gentleman from California, for an opening statement.

Mr. LUNGREN. Thank you very much, Madam Chairwoman. And I noted you talked about the possible and the impossible. It may be impossible for us to hold this hearing because of all of the comings and goings that we are having on the floor of the House today, and if we could just get the germaneness rule figured out between now and the end of the day, we might be able to get back to regular work.

I thank you for holding this hearing, and I welcome the opportunity to discuss foreign ownership and foreign investment, its impact on the critical infrastructure of the country.

This Homeland Security Committee is all too familiar with the concerns and fears that foreign ownership of U.S. critical infrastructure assets create in our citizens. The 2006 purchase of the operating rights at six U.S. ports, including the Ports of New York, New Jersey, and Baltimore by the Dubai Ports World Company, owned by the UAE, created a firestorm of public and congressional opposition. I may be one of the few Members of Congress who was

not so worried at the time. Perhaps because I was born and raised in a large port city, the city of Long Beach, California, and for 10 years represented both Long Beach and L.A. ports, it had dawned on me at an early age that ports had foreign ships, foreign workers, and foreign investment; and without that foreign investment in our ports of the United States, we would not be in as good shape as we were otherwise.

I was one of those who thought that it is good that people think it is good to be investing in the United States. I would rather have them think this is the place to invest than somewhere else. But nonetheless, the Dubai Ports World controversy focused attention on the governmental process established to review such sales and determine whether review protects our economic and national security.

Of course, I am referring to the CFIUS, or Committee on Financial Investment in the United States.

Amid growing concerns over foreign acquisition of American businesses in 1988—that was my last year in Congress during my first tour of duty here—Congress passed the Exon-Florio provision, which gives the President the authority to block proposed foreign acquisitions that threaten our national security. Foreign acquisitions of U.S. Government assets do pose a challenge to our government. It does create a delicate balancing act in the worldwide economy. How do we attract vital foreign investment to the U.S. without sacrificing or diminishing our national security?

I do believe we have the proper procedures in place to protect our critical infrastructure and assets by requiring foreign acquisition to be closely reviewed and scrutinized by CFIUS.

For over 30 years, this process has worked effectively, guarding our capital markets, our high-valued infrastructure assets, and most importantly, our national security. On only one occasion of which I am aware, in 1990, the President intervened and ordered a divestiture by a Chinese aerospace company of a U.S. aircraft parts manufacturer.

Last year's debate on the Dubai purchase raised a number of problems with the CFIUS review process. It demonstrates the changes needed to be made in light of 9/11 and our Nation's growing concern for security.

I believe important improvements were included in the legislation we passed last year, H.R.µ5337, and again in February of this year, H.R. 556, at that time by a vote of 423 to zero.

One of the important things it does is, it elevates the Secretaries of Homeland Security and Commerce to Vice Chairs of CFIUS, which will ensure a broader definition of national security threats in the CFIUS review. This legislation also limits delegating these important CFIUS decisions below the under secretary level.

I would just say with respect to American businesses that operate overseas or bring some of their corporate structure overseas, it is important for us to see how they protect assets that we don't want to be revealed to others. But this is not something new; this is what we did throughout the entire Cold War. And then, in some cases, the most important technology we were working with were computers, but it also had to do with things as mundane as that which we used for offshore drilling, that which we used for explo-

ration of oil around the world. We believed that some of those things ought to be limited at that time because of it.

But we have to remember how fast the world works. I can remember back in the 1980s, when we had something called a global positioning satellite as a DOD project, and they were coming around telling us that we ought to vote for it because it would allow us to be able to determine where our military people were, within 100 feet of where they were. For Mother's Day, I just bought my wife a GPS. That shows how fast that which we want to protect from suspicious eyes of others become commonplace.

So that is the challenge we have, and I would be very interested to find out how we deal with that from the standpoint of our witnesses.

And I thank the gentlelady for yielding me this time.

Ms. JACKSON LEE. I thank the gentleman for his remarks.

Other members of the subcommittee will be reminded, under the committee rules, opening statements may be submitted for the record.

Ms. JACKSON LEE. At this time I would like to welcome our panel of witnesses.

Our first witness will be Mr. Richard T. Garcia, Global Security Advisor, Corporate Affairs Security, Shell International.

Mr. Garcia began his position on August 1, 2005, after retiring from the Federal Bureau of Investigation with 25 years of service as the Assistant Director for the Los Angeles field office.

Welcome, Mr. Garcia.

As the Global Security Advisor, Mr. Garcia coordinates with other intelligence and law enforcement agencies, both domestic and foreign, in an effort to obtain strategic intelligence regarding potential criminal terrorist attacks against Shell assets globally.

Mr. Garcia also manages security advisors in North America and in Latin America, as well as the intelligence and assessment team with offices in Washington, D.C., and London.

Our second witness is Mr. Michael Pfister, Senior Vice President and Chief Information Officer at Halliburton. Mr. Pfister was named Senior Vice President and Chief Information Officer for Halliburton in January 2007. Previously, Mr. Pfister was President and Chief Operating Officer in a privately held health care firm in New Braunfels, Texas.

The final witness of this panel is David Marchick, Partner at Covington & Burling. Mr. Marchick's practice focuses on complex international trade, investment, transportation and legislative matters. Mr. Marchick is also a leading expert on the Exon-Florio amendment and has an active practice advising U.S. and foreign companies on security approvals from the Committee on Foreign Investment in the United States.

He is a coauthor of the book, National Security in Foreign Direct Investments. He has testified in Congress on numerous occasions on implementation of the legislation and played an active role in congressional consideration of the legislation that would amend the legislation in question.

Without objection, the witnesses' full statements will be inserted in the record.

I now ask each witness to summarize his statement for 5 minutes, beginning with Mr. Garcia from Shell, if you would.

STATEMENT OF RICHARD T. GARCIA, GLOBAL SECURITY ADVISOR, CORPORATE AFFAIRS SECURITY, SHELL INTERNATIONAL

Mr. GARCIA. Madam Chair, members of the subcommittee, I am pleased to appear before you today to testify on the impacts of foreign ownership investment and the security of our Nation's infrastructure.

Shell is active in more than 130 countries with 109,000 employees worldwide. Security plays a vital role in every one of our operations. When we operate politically in stable, geologically challenging regions, leading-edge security is critical to our success. Shell has a century-old history in the United States; one-third of Shell's assets and shareholders are here in the United States.

Shell Oil Company, through its U.S. affiliates, owns more than 10,000 miles of pipeline, 59 product terminals, nearly 1,000 storage tanks, as well as chemical facilities and oil refineries. Shell U.S. operates oil and gas rigs onshore and offshore around the country. We have 22,000 people working in Shell offices from New York to Los Angeles, from the Arctic Circle to the Gulf of Mexico. We invest heavily in the personnel training systems and tools we need to protect our people and our assets.

Since September 11th of 2001, Shell has invested in facility protection, training, access monitoring, and communications. Since 9/11, we have brought people into our corporate affairs security office from the Federal Government, law enforcement, military, and the Coast Guard. Shell U.S. maintains strong ties with these and other agencies that allow us to share information.

We also receive briefings from DHS and the State Department's Overseas Security Advisory Council on security issues important to Shell in the energy industry.

Our security team participates in various information-sharing programs from the U.S. Government such as the FBI's Texas coastal regional alert system, the intelligence of terrorism network, which work with our information-sharing programs in Houston and Los Angeles.

We also participate in the FBI's information-sharing program, which is currently where I am a member of the national board.

Shell Oil Company, which operates in the United States, is a subsidiary of the Royal Dutch/Shell Group, a group global company incorporated in the United Kingdom and headquartered in the Netherlands.

I am here today because you would like Shell's perspective on how foreign ownership or foreign investment impacts critical infrastructure. Let me say, as far as Shell is concerned, it does not affect us. I am aware of no instance where our foreign ownership or foreign investment has had any negative impact on keeping Shell's infrastructure and keeping it safe. I believe our energy infrastructure is secure as it would be as if Royal Dutch/Shell were based here in the United States.

A diplomatic relationship between the United States and the Netherlands is one of the strongest unbroken relationships in the

world. The Netherlands was the first country to recognize the American flag in November 1776, only 4 months after we declared independence.

Shell has always had strong security measures in place protecting our people and infrastructure. Within months of 9/11, the oil and gas industry developed security protocols and procedures for all segments of the industry, including pipelines and terminals. Shell participates fully with the Homeland Security Information Network, which allows DHS to get information quickly and easily to those responsible for the security of critical infrastructure.

Shell also participates fully in Homeport. Homeport has the same function, but is focused on the maritime aspect of the critical infrastructure, facilities with docks and wharves. It is a Web-based portal for industry to access necessary information or for the Coast Guard to push data quickly should a threat materialize.

As you may be aware, the Federal Government has also developed a credentialing program which will document transportation workers who have access to sensitive areas and equipment.

In addition, Shell maintains a global network and helps with the relationship between the government and agencies around the world to protect our people and assets because a threat to our infrastructure is as likely to come from the outside as it is to come from inside. Shell's network helps us protect our U.S. infrastructure.

Finally, Shell's security measures here are strengthened by the challenges being encountered around the world. Shell's experience in keeping our people and our assets secure in politically unstable regions and difficult climates sharpens our expertise in keeping our people and our assets safe here in the U.S. What we learn around the world, we apply here.

Shell is proudest of the safety and reliability of our U.S. infrastructure, and it remains dedicated and committed to our security.

Thank you for allowing me to be here to answer the questions that you.

[The statement of Mr. Garcia follows:]

PREPARED STATEMENT OF RICHARD T. GARCIA

Chairwoman Jackson-Lee, Ranking Member Lungren and Members of the Subcommittee: My name is Richard Garcia and I am an employee of Shell Oil Company and serve as the Global Security Advisor for Shell International. In that capacity, I coordinate with law enforcement agencies in the United States and abroad to prevent attacks—both criminal and terrorist—against Shell's personnel or assets. I manage Shell's security advisors in North and Latin America. I also direct Shell's Information and Assessment Team, which has offices in Washington, D.C. and London. Prior to joining Shell, I was with the FBI for 25 years. I headed both the Houston and Los Angeles FBI field offices.

I am pleased to appear before you today to testify on the impact of foreign ownership and foreign investment on the security of U.S. infrastructure.

Shell is committed to protecting our assets and our people around the world. Shell companies produce oil, gas, chemicals, lubricants and alternative energies like wind and hydrogen around the globe. Security plays a vital role in every one of our operations. When we operate in politically unstable or geologically challenging regions, security is mission critical to our success.

Shell has a century-old history in the United States. One third of Shell's assets, and shareholders are here in the United States. Shell Oil Company, through its U.S. affiliates, (Shell US) owns and operates 5,000 miles of pipeline and has partial ownership of 10,500 miles of pipeline. We wholly or partially own 59 products terminals and 960 storage tanks with more than 67.8 million barrels of capacity.

Shell US owns and operates five refineries in the United States with a combined capacity of 753,000 barrels per day. Six plants produce 15 billion pounds of chemicals annually for industrial use. Seven blending and packaging facilities around the country prepare our automotive consumer products like engine oils and lubricants. Shell US operates oil and gas rigs onshore and offshore around the country. We have 22,000 employees working at Shell sites and Shell offices from New York to Los Angeles and from the Arctic Circle to the Gulf of Mexico.

Shell US invests heavily in the training, employees, systems and tools we need to protect our people and our assets. Since September 11, 2001, we have invested in facility protection, training and communications all the way from wellheads and offshore platforms to tankers, ports, pipelines, refineries and storage tanks.

All of these steps were carried out in close partnerships with law enforcement and security officials. Shell US maintains strong relationships with federal, state and local law enforcement agencies in the United States. Shell hires skilled security professionals who have the experience, training and professional relationships to protect Shell's people and infrastructure.

Note: The companies in which Royal Dutch Shell plc directly and indirectly owns investments are separate entities. In this Statement, the expressions ''Shell'', ''Group'' and ''Shell Group'' are sometimes used for convenience where references are made to Group companies in general. Likewise, the words ''we'', ''us'' and ''our'' are also used to refer to Group companies in general or those who work for them. These expressions are also used where there is no purpose in identifying specific companies.

Since 9–ll, Shell Oil Company has recruited professionals into our Corporate Affairs Security office from the State Department, the police and military and the Coast Guard. Shell US maintains strong ties with these and other agencies that allow us to share information back and forth. Shell Oil Company's security team also receives briefings from Department of Homeland Security (DHS) and the State Department's Overseas Security Advisory Council on security issues important to Shell and the energy industry.

The U.S. security team participates in various information-sharing programs from the U.S. Government such as the FBI's Texas Coastal Regional Alert System and the Intelligence and Terrorism Alert Network, which are information-sharing programs in Houston and Los Angeles. In my previous employment with the FBI, I was responsible for the expansion and enhancement of these two programs. The U.S. Security team also participates with the FBI's InfraGard information sharing program where I am currently on the National Board of Directors for InfraGard.

Shell Oil Company, which operates in the United States, is a subsidiary the Royal Dutch Shell Group, a global energy company incorporated in the United Kingdom and headquartered in The Netherlands.

I am here today because you would like Shell's perspective on whether foreign ownership or foreign investment impacts the security of critical infrastructure. Let me say simply: It does not. I am aware of no instance where our foreign ownership or foreign investment has had any negative impact on keeping Shell's infrastructure and people safe in the United States. I believe our energy infrastructure is as secure as it would be if Royal Dutch Shell plc were headquartered here in the United States.

The Dutch-American friendship goes back more than 200 years. The Netherlands was the first country to recognize the American flag in November 1776—four months after our nation declared independence. The diplomatic relationship between the United States and The Netherlands is one of the longest, unbroken diplomatic relationships in the world.

Before 9–11, She had strong security measures in place to protect our people and infrastructure. But the world of corporate security changed forever on 9/11, as we had to more seriously address the possibility of intentional acts to harm our facilities and employees instead of just accidental events. Since 9–11, the oil and gas industry has forged a partnership with government at all levels to protect hundreds of facilities across the country from the potential of terrorist attacks. Shell is a full participant in that partnership.

Within months of the attack, the oil and gas industry developed security measures for all segments of the oil and gas network—including pipelines, refineries, terminals, and others. The American Petroleum Institute and the National Petrochemical and Refiners Association produced an industry-wide method for managers to identify security vulnerabilities in their operations. The Security Vulnerability Assessment methodology is a sophisticated, risk-based tool used to identify the security hazards, threats and vulnerabilities of a facility, and to evaluate the best measures to provide secure facility operations. In other words, it provides the framework for a complete security analysis of the facility and its operations. The SVA covers both

physical and cyber security, process safety, facility and process design and operations, emergency response, management and law enforcement.

In 2004, the oil and natural gas industry expanded the SVA methodology to include pipeline, truck, rail and liquefied natural gas (LNG) operations. DHS has recognized the SVA methodology and even uses it to train its own employees and Shell US has provided personnel to DHS to assist in this training. Shell US has participated fully in the use and expansion of the SVA methodology.

The oil and gas industry and federal security personnel also completed the "Security Guidelines for the Petroleum Industry," to help employers protect facilities and respond to changes in the threat level. This guidance is now in routine use as a roadmap for companies in deciding how best to protect all sectors of the industry against the threat of attack. These are the working methods and countermeasures the oil sector uses to protect all segments of the industry.

The guidelines are important because they allow companies to manage security risks and provide a reference to federal security laws and regulations that have an impact on petroleum operations. The Secretary of Energy and later the Undersecretary for the Department of Homeland Security have endorsed the industry guidelines. These security protocols are constantly being updated. A third edition was published in April 2005. Shell continues to use these guidelines.

As you may be aware, a new program currently being developed by the US Government will aid in securing certain Shell US facilities even further by the implementation of the Transportation Worker Identification Credential (TWIC). With the TWIC program, appropriate government background checks can be conducted to aid in identifying the insider threat to Shell US facilities by properly clearing the workers who have access to sensitive areas and equipment.

Shell US participates in the Homeland Security Information Network. HSIN is a web-based portal that allows DHS to pass security related information to the Critical Infrastructure Community. It is managed by DHS. All members must be vetted by the Oil and Gas Sector Committee of the DHS to be admitted. HSIN allows DHS to push data to the sector quickly and easily.

Shell also participates fully in Homeport. Homeport has the same function but is focused on the maritime aspect of the critical infrastructure, facilities with docks and wharves. It is a web-based portal for industry to access necessary information or for the Coast Guard to push data should a threat materialize.

Membership in HSIN is focused at the corporate level for Shell whereas Homeport is geared to the facility owner and operator.

In addition to Shell US' extensive security work within the oil and gas industry and with law enforcement agencies, Shell has built a global network that allows us to leverage our relationships with governments and law enforcement agencies around the world to protect Shell employees and assets. We exchange information, forge partnerships, design systems and implement procedures in partnership with governments and companies in other countries just as we do here. Because a threat to our U.S. infrastructure is as likely to come from outside the United States, as it is to come from the inside, Shell's network helps us protect our U.S. infrastructure.

Finally, Shell's security measures in the United States are strengthened by the challenges we encounter around in the world. Shell's experience in keeping our people and our assets secure in politically unstable region, geologically-challenging areas and difficult climates sharpens our expertise in keeping our people and infrastructure safe here in the United States. What we learn around the world we apply here, just as what we learn here we apply around the world. I believe Shell's global presence strengthens the security of our U.S. assets.

Shell is committed to providing a reliable supply of fuels and products to keep the economy growing. We are proud of the reliability of our oil and gas infrastructure and remain committed to its security. Thank you.

Ms. JACKSON LEE. We are going to try to have you begin your testimony and then recess after your testimony.

Mr. Marchick, if you will be patient, we would appreciate it; and Mr. Ranking Member, I would like to ask unanimous consent that we could continue this hearing without a quorum so we can at least get through.

Mr. LUNGREN. Thanks.

STATEMENT OF MICHAEL PFISTER, SENIOR VICE PRESIDENT AND CHIEF INFORMATION OFFICER, HALLIBURTON

Mr. PFISTER. Thank you, Chairwoman Jackson Lee and Ranking Member Lungren, members of the Committee on Homeland Security.

I am Michael Pfister, Senior Vice President and Chief Information Officer of Halliburton Company. I am here today to witness on behalf of Halliburton Company, founded by Earl P. Halliburton in 1919 and incorporated in the State of Delaware.

Halliburton received correspondence by committee Chairman Bennie Thompson, offering us an opportunity to testify before this committee. That correspondence indicated that the topic of the hearing would be the impact of foreign ownership and foreign investment on the security of our Nation's critical infrastructure.

Halliburton is not foreign owned, and we do not possess critical infrastructure as we understand it. However, we would like to be of whatever help we can to this committee, and we might be of assistance relative to your introduction if we describe how we protect our technology and our information from being obtained and used by those who might wish to do our country harm.

Halliburton and the energy industry for some time have been responding to the reality of the global business environment for which key employees travel around the world and need to have access to very sensitive information in order to do their jobs correctly. It also a given in today's world that threats to the security of vital information comes from almost every location around the globe. Hackers do not need to be near important computer resources.

The IT security landscape for Halliburton assumes that all of our important IT assets, regardless of which data center they are located in, are under constant attack by hackers from every location around the globe. In fact, in our world, we intercept 16,000 viruses every day, and we respond to about 12,000 attacks per day upon our network perimeter. So we have no choice but to take this information—information security extremely seriously.

The IT industry has established security standards practiced by the Federal Government and by corporations like us that protect the perimeters of our networks, that protect the transmission of our information through public carriers, and it protects the centers that host the servers that run our applications and store our important raw data.

Like the rest of the energy sector, Halliburton's IT security relies on what we call defense in depth. It is multiple layers of defense that are placed throughout the IT system, and the idea behind this defense in depth is the idea that any attacker would have to break through multiple defensive countermeasures in order to successfully hack into the system.

Modeled much after the security systems that have evolved over the years, Halliburton operates industry standard firewalls, antivirus and intruder prevention systems to separate our internal network and all of the information on it from the Internet. We perform perimeter audits to ensure that our firewalls are doing their jobs. We regularly monitor for suspicious activity, and we isolate that activity before it can do any harm.

We utilize third-party security experts to test our security systems' effectiveness, and we encrypt our digital communications before we transport them through public communication networks.

In addition to all of the technical security we deploy to protect our information assets, there are other steps taken by Halliburton to physically secure its confidential data and its facilities. Our facilities have physical barriers such as fencing, locked doors, locked traffic gates. We employ security guards to prevent unauthorized access and entry to both tangible and intangible property. We restrict access to our facilities to persons having proper credentials, such as electronic badges, and badge access records are automatically retained and maintained and reviewed from time to time. Visitors to our Halliburton facilities are required to sign in and are escorted as they make their way through our facilities.

We store our trade secret information, such as drawings and specifications that make us competitive, in a digital vault that is referred to as the matrix database. And the control access to this important trade secret information, the matrix database, recognizes the degree of authorization that has been granted to a user, and it appropriately limits the user's access to authorize data in the system.

In addition, there are federally mandated export controls that impact our security assets as well. Halliburton has complex procedures in place to manage the export of our company's technical data. These movements are screened either through our company's system or by a member of the law department's trade compliance group. And in doing so, we believe that we may be helping to protect our country's critical infrastructure while keeping assets out of the hands of individuals who should not have them.

There is also a need in our business to control to the best of our ability, the activities of employees that are entering and leaving our company.

We have thousands of patents and many skills that we use to remain one of the finest energy service companies in the world. In our industry, there is a fairly constant turnover rate of talented and educated individuals, and for that reason, we have developed the following methods to protect Halliburton's intellectual property: new employee packages, provided by our H.R. department, include an intellectual property assignment and a confidentiality agreement that requires the employee to assign to Halliburton any IT that was developed during his employment and that relates to company business, and to maintain the secrecy and the confidentiality of any information to which they might have been exposed.

Ms. JACKSON LEE. Your time has expired.

Would you be kind enough to summarize or respond to our questions?

Mr. PFISTER. I want to close by saying that our success depends upon a well-trained workforce. We provide a bunch of training options to teach people how to take good care of our proprietary information. Some of them are online; others are instructor-led.

I want to thank you for allowing me to appear here today, and I hope that we have provided some information that will be of help to the committee. We take very seriously our responsibility for protecting data and trade secrets and intellectual property.

I will be happy to answer any questions after we get done, and if I don't possess the information, we will get it for you for the record.

[The statement of Mr. Pfister follows:]

PREPARED STATEMENT OF MICHAEL PFISTER

Chairwoman Jackson–Lee, members of the Committee on Homeland Security, I am Mike Pfister, Senior Vice President and Chief Information Officer of Halliburton Company. I am here today as a witness on behalf of Halliburton Company, founded by Earl P. Halliburton in 1919 and incorporated in Delaware. Halliburton received correspondence on May 9th from Committee Chairman, Congressman Bennie Thompson, offering us an opportunity to testify before this committee. That correspondence indicated that the topic of the hearing would be "The Impact of Foreign Ownership and Foreign Investment on the Security of Our Nation's Critical Infrastructure." Halliburton is not foreign owned and does not possess critical infrastructure. However, we would like to be of whatever help we can to this committee and I believe that we might be able to be of assistance if we describe how we protect our technology and information from being obtained and used by those who might wish to do our country harm. With that in mind, I would like to take a few minutes of your time to address Halliburton's Information Technology and the safeguards we employ to protect our assets.

Halliburton, and the energy industry—along with the Information Technology (IT) industries—have, for some time, been responding to the reality of a global business environment in which key employees travel around the world and need to have access to very sensitive information in order to do their job correctly. It is also a given in today's world that threats to the security of vital business information come from almost every location around the globe. Hackers do not need to be near important computing resources. They take the path of least resistance and use the power of the Internet to locate information, regardless of where in the world it might be. The frequency and approaches that they use are independent of where key information stores reside, or where key employees office. For that reason, international business companies that have key corporate leaders, such as our CEO, Mr. Dave Lesar, who spend significant time outside the borders of the United States do not materially increase the risk that through IT methods, important information might be compromised. The IT security landscape for Halliburton assumes that "all important IT assets", regardless of which data center they are located in, are under constant attack by hackers from every location. That assumption is already in place, and preventive security measures are geared to that reality, regardless of where key employees are at any moment.

Our customers do control most of the critical energy infrastructure and we have worked with those customers and IT security vendors to develop robust products and approaches to protect the information stored in our databases and other data repositories. The IT industry has established security standards, practiced by the federal government and by corporations, that protect the perimeters of our networks, the transmission of our information through public carriers, and the centers that host the servers that run our applications and store our raw data.

Like the rest of the energy sector, Halliburton's IT Security relies on "Defense in Depth"—multiple layers of defense are placed throughout an IT system and address personnel, technology, and operations for the duration of the system's lifecycle. The idea behind the Defense in Depth approach is that any attacker should have to break through multiple defensive countermeasures, in order to successfully hack into the system. This increases the likelihood of being able to identify and prevent an attack from occurring.

Halliburton operates industry—standard firewalls, antivirus, and intrusion prevention systems to separate our internal network from the Internet. Halliburton performs perimeter audits to ensure the firewalls are doing their jobs. We regularly monitor for suspicious activity and isolate that activity before it can do any harm. We utilize third party security experts to test our security system's effectiveness. We encrypt digital communications before transporting them through public communications networks.

It is worth noting at this point that the energy sector participates in the National Infrastructure Protection Plan. There is a sector-focused project called LOGIIC (Linking the Oil and Gas Industry to Improve Cyber Security). However, its focus has been on Supervisory Control and Data Acquisition (SCADA) and other "control systems" that control production and distribution of hydrocarbons. Halliburton does not operate these systems. We also share industry best practices each quarter

VerDate Nov 24 2008 08:36 Jun 25, 2009 Jkt 000000 PO 00000 Frm 00016 Fmt 6633 Sfmt 6621 H:\DOCS\110-HRGS\110-36\48911.TXT HSEC PsN: DIANE

through the American Petroleum Institute's Information Technology Security Forum.

In additional to all the technical security we deploy to protect our information assets, there are other steps taken by Halliburton to physically secure its confidential data and its facilities.

- Halliburton facilities have physical barriers (fencing, locked doors, and locked traffic gates) and security guards to prevent unauthorized entry and access to both tangible and intangible property.
- Halliburton restricts access to facilities to persons having proper credentials, such as electronic badges. Badge access records are automatically made and maintained.
- Visitors to Halliburton facilities are required to sign-in and then are escorted throughout the facility.
- Halliburton marks certain documents as "confidential" or uses other appropriate headers / legends when such documents contain confidential information of the company.
- Warning labels appear on computer log-in screens to inform users that the system contains business confidential information and is for company use.
- Halliburton stores trade secret information (drawings, specifications, etc.) in an electronic vault that is referred to as the Matrix database. To control access to the trade secret information, the Matrix database recognizes the degree of authorization that has been granted to a user and appropriately limits the user's access to authorized data in the system.

Our internal controls over our own vital assets are engendered largely to keep us competitive with others in the energy service field and of the most benefit to our clients. However, there are federally mandated export controls that impact our security practices as well. Halliburton has procedures in place to screen the export of our Company's technical data. These movements are screened either through the Company's SAP system or manually by a member of the Law Department's Trade Compliance Group. In so doing, we believe we may be helping to protect critical infrastructure while keeping assets out of the hands of individuals that should not have them.

So, I hope this brief technical disclosure helps this committee to appreciate the significant investment that we have made to protect information about our business from those with bad intentions.

There is also a need in our business to control, to the best of our ability, the activities of employees that are entering and leaving the company. We have thousands of patents and many skills that we use to remain one of the finest energy service companies in the world.

In our industry, there is a fairly constant turn over rate of very talented and educated individuals. For that reason, we have developed the following methods to protect Halliburton's intellectual property.

New employee packages provided by Halliburton's Human Resources (HR) department include an intellectual property assignment and confidentiality agreement that requires the employee to assign to Halliburton intellectual property developed during his/her employment that relates to company business; and to maintain the secrecy of proprietary confidential information he/she develops or to which he/she is exposed.

When an employee who had access to Halliburton's valuable proprietary information leaves the company, Halliburton's Law Department works closely with the HR Department and the business units, seeking to prevent the employee from taking that information for his or her own benefit or that of another, e.g., a competitor. When appropriate, access to our computer systems is disabled immediately. At other times during exit interviews, key employees are reminded of their continuing obligations under any applicable intellectual property and confidentiality agreements, and are requested to return any Halliburton proprietary information in their possession. When circumstances warrant, the company will send a letter to the departing employee, and possibly his new employer, formally reminding the ex-employee of his obligations to the company. If Halliburton suspects that the departing employee intends to or will be in a position to use Halliburton information in violation of those obligations, the company will consider taking legal action against the ex-employee and other responsible parties. There is a Dispute Resolution Agreement in place between the company and its employees that normally will require such disputes with ex-employees to be submitted to binding arbitration.

In addition, when Halliburton engages a third party to provide goods or services and Halliburton is required to disclose confidential information to the third party, the third party is contractually obligated to maintain the confidentiality of such information. Typically, when a third party is engaged in Halliburton technology devel-

opment, all rights to the developed technology are assigned to Halliburton, and again, the third party is required to maintain the confidentiality of Halliburton's proprietary information. In some cases, the developed technology could be jointly owned by Halliburton and a co-developer, but in those cases as well, the parties will be obligated to maintain the confidentiality of proprietary information shared by one with the other.

The company provides a number of courses in its "I-Learn" catalog that relate to protecting Halliburton's valuable proprietary information, and to the proper handling of confidential information of third parties that is lawfully in the company's possession. Some of these courses are fully electronic, or on-line; others are instructor-led. The "I-Learn" system has been developed by Halliburton to allow its employees to easily learn about many topics often while sitting in the comfort of their own offices.

I again thank you for allowing me to appear here today and hopefully I have provided information that will be of help to this committee. I would be happy to answer any questions you might have and if I do not posses the information you want with me today, I will be happy to provide it for your record.

Ms. JACKSON LEE. Thank you very much.

The committee stands in recess.

[Recess.]

Ms. JACKSON LEE. Thank you.

Mr. Marchick, would you please begin your testimony?

STATEMENT OF DAVID MARCHICK, COVINGTON & BURLING LLP

Mr. MARCHICK. Thank you, Madam Chairman, and it is a pleasure to be here. I know from personal meetings with you how much you have focused on this issue, how deeply you have investigated this issue, and I appreciate the leadership you have shown on this. I would like to make four points, Madam Chair.

The first is that we want more foreign investment, not less. Foreign investment is part of the lifeblood of the U.S. economy. Employees, foreign companies employ about 5 million Americans, paying higher wage jobs than American-owned companies. It is critical to our technology and manufacturing base. Foreign-owned companies own about 5µpercent of all U.S. assets, but they employ about 20µpercent of all manufacturing jobs, so it is critical to our manufacturing base. And as long as we spend more than we save, we need the money to come from somewhere, and it is better for foreign entities to invest in fixed assets than in liquid assets because you simply can't dump fixed assets like you can liquid assets. So we want them to invest. It is good for our economy. It is good for R&D.

Second is the issue of critical infrastructure. This committee, the Homeland Security Department and its predecessors, going back for almost 15 years, have really struggled with the concept of what critical infrastructure is. During the Clinton administration, the Clinton administration put out a study that the critical infrastructure covers about eight sectors. In 2001, Congress passed the PATRIOT Act and defined critical infrastructure as systems and assets that are so vital to the U.S. national and economic security that their destruction would have a debilitating impact on U.S. national security.

Since that time, there have been four different reports that have come out from the executive branch with four different definitions of critical infrastructure and four different lists of sectors.

Now why is this important? It is important because investors and security managers, like Mr. Garcia, take guidance from the government on what is critical infrastructure and what is not; and foreign investors take guidance on that as well. And so, unless there is clear guidance from the government as to what critical infrastructure is, it will make it more difficult and there will be more insufficiency for investors in deciding whether to invest with the United States. Because if a transaction—if a foreign investment implicates or covers critical infrastructure, then there is a greater likelihood that it has to go through the CFIUS review process. And if companies don't know whether they have to go through that process, it creates uncertainty, and uncertainty chills investment.

So the third issue is that the CFIUS process since Dubai Ports has changed significantly. Transactions are now regularly going to very, very high levels in the government, sometimes all the way up to the Secretary, sometimes all the way up to the President, there is additional scrutiny. There has been an increase in the number of mitigation agreements or conditions imposed by the government.

The Homeland Security Department has taken a very active role in this. Last year they negotiated—they required companies to commit to 15 mitigation agreements, which is three times the number of agreements required the previous year and equal to all of the mitigation agreements in the previous 3 years.

So, as a result of the increased oversight from this committee and others, there has been additional scrutiny of foreign investments in the United States.

Frankly, in my view, not all of that is good, because overregulating investment has a chilling impact; and I know, from my practice, that there are investors who have decided not to pursue investments because of the CFIUS process. So the balance, the pendulum shifted dramatically after the Dubai Ports controversy, and hopefully that pendulum will swing back towards the middle.

The final issue is legislation. Mr. Frank and Mr. Bachus and the Financial Services Committee put together a very good bill with Mrs. Maloney and Ms. Pryce. This committee and Chairman Thompson and Mr. King played a very important role in shaping that legislation; they were original cosponsors.

You and Mr. Lungren played a very important role as well. It gives the Homeland Security Department additional authority. That legislation, I think, is very good legislation. It passed unanimously in the House.

Today, in the Senate, Senator Dodd and Senator Shelby marked up similar legislation based on the House bill with a few changes. Hopefully, that will go through the Senate quickly and come back to the House with a conference, and hopefully, we can get a good bill.

That legislation further increases the scrutiny that transactions will have to go through under the CFIUS process. It requires additional scrutiny of government-owned acquisitions. It requires additional reporting to Congress; Congress will have a much greater oversight role. And it requires additional factors to be considered

VerDate Nov 24 2008 08:36 Jun 25, 2009 Jkt 000000 PO 00000 Frm 00019 Fmt 6633 Sfmt 6601 H:\DOCS\110-HRGS\110-36\48911.TXT HSEC PsN: DIANE

in every transaction, factors that now are much more relevant after September 11th including investment in critical infrastructure.

So the hearing that you are pursuing today is a very important hearing. Congressional oversight is very important, and the most important thing is that, through hearings like this, there is additional confidence in the integrity of the CFIUS process, so we don't have another Dubai Ports, which is not good for our country and not good for our relationships with other countries.

[The statement of Mr. Marchick follows:]

PREPARED STATEMENT OF DAVID MARCHICK [1]

Chairman Jackson-Lee and Ranking Member Lungren

Thank you for the opportunity to testify before your committee today on the important subject of foreign ownership of critical infrastructure.

I plan to discuss three issues in my testimony:

First, the concept of "critical infrastructure" and the implications of foreign ownership thereof;

Second, recent developments in the Committee on Foreign Investment in the United States;

Third, CFIUS-reform legislation moving through the Congress.

Foreign Ownership of Critical Infrastructure

A significant amount of work has been undertaken in this Committee, in the Department of Homeland Security and its predecessor agencies, and in the private sector with respect to defining and protecting critical infrastructure. This work dates back to the mid–1980s and continues to evolve today.

There have been many iterations of the government's definition of "critical infrastructure" over the years. In 1996, for example, President Clinton issued Executive Order 13010, which stated that "certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States." EO 13010 listed eight sectors as critical infrastructure, including telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, and transportation.

Building on this initial concept, the USA PATRIOT Act, and later the Homeland Security Act, defined "critical infrastructure" as:

> "[S]ystems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." [2]

This definition, by setting a high threshold, implies that a relatively narrow list of assets would be deemed to "have a debilitating effect." Core communications assets or the electrical grid certainly would meet this definition. But in the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, the White House identified twelve very broad sectors as critical infrastructure, including agriculture and food, water, and public health.[3] In the book that I co-authored with Monty Graham of the Peterson Institute, Mr. Graham estimated that these twelve sectors cover some 25% of U.S. employment.[4] Taking this effort one step further, the Department of Homeland Security created a "national assets database," which contains tens of thousands of entries compiled from various sources, including state and local officials. The Information Assurance and Infrastructure Protection Division of DHS reported that it had identified 1,700 "critical assets" in 2004. And since

---

[1] David Marchick is a partner at Covington & Burling LLP, a Washington-based law firm. He has an active CFIUS practice and is co-authored the book "U.S. National Security and Foreign Direct Investment (Peterson Institute, May 2006). Mr. Marchick represents U.S. and foreign investors before the Committee on Foreign Investment in the United States and the Congress. The views in this testimony are Mr. Marchick's views and not those of Covington & Burling LLP or the firms clients.

[2] Section 1016(e) of the USA PATRIOT Act, codified at 42 U.S.C. § 5195c.

[3] *See* National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, (February 2003), *available at www.*whitehouse.gov (last visited May 20, 2006).

[4] *U.S. National Security and Foreign Direct Investment,* by Edward M. Graham and David M. Marchick, Peterson Institute, May 2006, p. 149.

2001, there have been four different executive orders or reports, each of which included *different* sectors as critical infrastructure.[5]

The definition of critical infrastructure matters because the private sector makes key decisions—investment and resource allocation decisions—based on guidance from the federal government. Yet the evolving and increasingly broad definition of critical infrastructure, coupled with little guidance from the government on the national security issues associated with investment and management of such infrastructure, has created ambiguity and uncertainty for U.S. companies looking to increase their value by attracting foreign partners as well as for direct foreign investors.

To be sure, we know from CFIUS practice, from statements by Homeland Security officials, and from H.R. 556 and the Dodd/Shelby bill, that protection of critical infrastructure is a top priority. And, for investment in certain sectors—including the defense industrial base, telecommunications carriers, and certain energy assets, including nuclear—there is a clear nexus to national security, there are established paradigms for assessing and, where necessary, mitigating national security risks posed by foreign investors. Foreign investors might reasonably expect to incur some national security-related mitigation costs associated with their investment in these sectors, and they should have some sense of what those costs will be (especially for investments in the defense industrial base where there are fairly standard terms for mitigation).

But these cases represent only a small percentage of investment in critical infrastructure, as that term has been broadly defined. It is far less clear that foreign ownership of other assets deemed to be "critical infrastructure" has any measurable impact on U.S. national and homeland security. Let me offer three examples of how the absence of guidance in this area is both troubling from a policy perspective and potentially costly in the marketplace.

First, there are certain areas of "critical infrastructure," broadly defined, that in the ordinary course simply should not raise national security concerns.

For example, there has been great controversy in certain states regarding the privatization of toll roads. While that debate is understandable, it would be far more difficult to see how foreign ownership of a toll road would raise national security issues. The same logic applies to most investments in agriculture and food. Ben and Jerry's is owned by a Dutch company, and Häagen-Dazs is owned by Diageo, a British company. I can think of many great ways to describe Cherry Garcia, but central to national security isn't one of them.

Second, regulations that preserve and protect the national interest already govern a number of sectors identified as "critical infrastructure." For example, there already exist myriad federal, state and local regulations to protect the food supply, to ensure the integrity of the banking system, and to facilitate high-quality public health services. This also is now true of investment in the chemical sector. Ambiguity as to whether investment in such sectors might also require a national security review because they technically are "critical infrastructure" unnecessarily complicates the investment and resource allocation calculus of both sellers and buyers.

Third, there is a real risk of "critical infrastructure" mission creep, particularly with respect to information technology products and services. Increasingly, in practice, the government is defining critical infrastructure to include not only the specifically identified sectors, but also any product or service sold into that sector. This produces a slippery analytic slope. An IT product that serves the exact same function for Ben & Jerry's as it does for AT&T may, because its customer is AT&T, be deemed part of critical infrastructure. This, in turn, creates unequal costs for foreign investors. For example, take two products that serve the same function on the IT networks of Ben & Jerry's and AT&T. Both products have source code that is written by engineers in Eastern Europe. Both products are incorporated into hardware assembled in China, with the hardware comprised of component parts made in a number of other countries all over the world. Both products are sold by publicly traded U.S. companies, and both companies use direct sales as well as distributors to reach their customers. One company is then bought by a foreign, publicly-traded company with no government ownership. Should that investment require a national security review simply because, among the many diverse customers of the product, some are located in "critical infrastructure" sectors?

To be sure, the answer to that question may be "yes" in some instances. Moreover, Exon-Florio and the CFIUS process can adequately identify and mitigate risks in those cases. However, even sophisticated counsel frequently have difficulty identi-

[5] *See,* E.O. 13228; the National Strategy for Homeland Security, July 2002; the National Strategy for Physical Infrastructure Protection, February 2003; and Homeland Security Presidential Directive 7, December 2003.

fying which instances these concerns may arise, or the potential costs associated with those issues. And this uncertainty is itself very costly, both for U.S. sellers who have an interest in creating the largest possible market for bidding and certainty with respect to closing, and for foreign investors who, in formulating their bid, must assess additional costs associated with their investment and how potential regulatory uncertainty both in timing and result might affect their competitive position vis-à-vis other bidders.

More can be done to provide clear guidance to foreign investors, U.S. companies and their investment advisors. While the definitions and classes of assets I described earlier may work for the *physical* protection of critical infrastructure, they do not work for foreign investment considerations. The Administration and Congress should work together to determine how best to protect critical infrastructure, regardless of who owns a particular company or asset. Security policies and guidance could be developed on a sector-by-sector basis. A baseline level of security requirements should be established. Then, if there are particular national security issues associated with foreign ownership in a particular asset, U.S. interests will be further preserved by CFIUS, which is well equipped to mitigate the risk or block the investment.

Recent Developments in CFIUS

Simultaneous with progress on CFIUS reform legislation in the Congress, CFIUS has undertaken a number of changes in response to concerns on the hill. These include:

- Committing additional resources to staffing CFIUS cases. Treasury has added a new CFIUS Deputy Assistant Secretary and DHS has added case officers and lawyers to focus on reviews and enforcement;
- Involving more senior level officials within CFIUS;
- Enhancing communications with Congress;
- Expanding coordination among intelligence agencies;
- Expanding the use of mitigation agreements and introducing new, tougher terms in such agreements; and,
- Enhancing enforcement of mitigation agreements, including through on-site audits and consultations with parties to such agreements.

In many respects, CFIUS has taken a much more cautious attitude toward their work post-DPW. This caution has had a ripple effect on the private sector, leading to more filings. In 2006, there were 113 filings (up 73 percent over 2005), 7 second-stage investigations (up 250 percent) and 5 withdrawals (up 150 percent) during the second-stage investigation period. A number of other transactions were withdrawn during the initial 30-day period. The dramatic increase in the number of second-stage investigations and withdrawals suggests that foreign investors are having a more difficult time closing transactions in a timely fashion. The stakes are high—the value of just one-third of the transactions that were submitted to CFIUS exceeded $95.5 billion in 2006.

CFIUS has also increased the number of "mitigation" or "national security" agreements negotiated as a condition for approval. From 2003–2005, the Department of Homeland Security (DHS) was a party to just 13 mitigation agreements, compared with 15 such agreements in 2006 alone. Foreign investors—particularly in the IT sector and other sectors considered "critical infrastructure"—now face a greater likelihood of being compelled to enter into a mitigation agreement in order to secure CFIUS approval.

The trend in filings has continued this year—there have been 54 to date, putting CFIUS on track for almost 150 filings this year, a 130 percent increase over 2005. Transactions that raise real national security issues should be filed and reviewed by CFIUS. But uncertainty about what cases should be filed will cause more transactions to be submitted for review than necessary. In turn, this forces CFIUS and the intelligence agencies to conduct a full analysis of inconsequential transactions, taking their focus off the transactions that really matter to national security. I suspect that over time this dramatic increase in filings post-DPW will level off to more normal levels, and that some caution in the agencies at this time is to be expected. The pendulum has swung too far post-DPW. For U.S. national security *and* economic interests, I hope the pendulum will soon swing back toward the middle.

Legislative Efforts to Amend Exon-Florio

In the wake of the Dubai Ports World controversy just over a year ago, more than 20 bills were introduced in the House and Senate that would have restricted or blocked foreign investment in one way or another. Certain of these bills would have simply prohibited foreign investment in critical infrastructure; others would have prohibited foreign government ownership of certain assets in the United States. Several bills would have amended Exon-Florio, the statute that gives the President the

power to block certain transactions that threaten U.S. national security. One bill amending Exon-Florio passed the House, and another passed the Senate, but the 109th Congress ran out of time before the bills could be reconciled.

On February 28, the House passed unanimously H.R. 556, the National Security Foreign Investment Reform and Strengthened Transparency Act of 2007, which was pulled together by Chairman Frank, Ranking Member Bachus, Congresswoman Maloney and Congresswoman Pryce, among others, and co-sponsored by Chairman Thompson and Ranking Member King of this committee. Today, in the Senate, Chairman Dodd and Ranking Member Shelby are marking up a bill based in large part upon H.R. 556.

Credit goes to you, Madame Chairman and Mr. Lundgren, and to Chairman Thompson and Mr. King, for helping to shape a bipartisan, balanced bill that enhances protection of national security while not impeding foreign investment in the United States. This Committee had an important role in shaping that legislation.

H.R. 556 would address many of the perceived shortcomings with the CFIUS process without chilling foreign investment. It would:

- Enhance Congressional oversight and reporting to Congress without politicizing transactions;
- Require higher-level involvement in CFIUS decisions;
- Expand the factors that CFIUS must consider to reflect post–September 11 imperatives, including protection of critical infrastructure;
- Heighten scrutiny for government-owned transactions without impeding investments that don't raise real national security issues; and,
- Allow for transactions to be reopened based on material intentional breaches of mitigation agreements where no other adequate remedy exists. This provision—the so-called "evergreen" provision—is tough medicine and a provision which foreign investors and key elements of the U.S. business community oppose.

Chairman Dodd and Senator Shelby are marking up a bill in the Senate Banking Committee that is substantially similar on H.R. 556, making some modifications that in my view are very good changes. Among other things, the Dodd/Shelby bill:

- Adopts the concept of rotating lead agencies and vests enhanced authority in those agencies to negotiate, monitor and enforce mitigation agreements. For example, DOD would take the lead on defense acquisitions; Homeland Security would lead on investments in ports, airports and transportation companies; Justice would take the lead where law enforcement issues were paramount; and Commerce would take the lead on transactions with significant export control issues;
- Eliminates some of the unnecessary bureaucratic provisions of H.R. 556, such as requiring two-thirds votes in CFIUS for certain decisions. Unlike Congressional committees, agencies don't typically vote; and,
- Imposes the same confidentiality requirements on Congress that exist within CFIUS.

I was pleased that the Senate decided to use the House bill as the baseline. If the Dodd/Shelby bill passes the Senate without significant changes, I am confident and hopeful that the House and the Senate could work together, in a bipartisan fashion, to send sensible CFIUS reform legislation to the President for signature.

The key, however, is that legislation advance U.S. national security interests without impeding foreign direct investment that we want and need. No bill would be better than a bad bill, but I am hopeful that the House and Senate can put together a good bill for the benefit of our economy and national security.

Conclusion

The United States very much needs additional investment in critical infrastructure from both domestic and foreign sources. The more investment, the more durable and resilient our telecommunications, energy and other critical infrastructure will be.

According to the Treasury Department:

- Foreign companies in the U.S. employed more than 5 million U.S. workers in 2005, providing 4.5% of all private sector employment in the United States.
- Manufacturing jobs accounted for 33% of the jobs created by foreign companies in the U.S. (2004 data).µ The manufacturing sector accounts for just 12% of overall U.S. private sector employment.µ Thus, FDI is disproportionately bolstering this important sector.
- An additional 4.6 million U.S. jobs indirectly depend on foreign investment in the U.S. (2005 data). Foreign companies in the U.S. buy 80% of their inputs from U.S. companies. This additional business indirectly supports almost as many U.S. jobs as FDI creates directly.

• Compensation at foreign companies in the U.S. is on average 30% higher than the U.S. national average.µ Foreign-owned firms paid U.S. workers an average of $63,428 in 2004.

Further, in 2000, foreign firms directly employed 5.7 million people in the U.S. (5.1% of the private sector workforce) and indirectly supported 6.5 million more jobs.µ In 2005, those figures had fallen to 5.1 million (4.7% of the private sector workforce) and 4.6 million, respectively.µ Foreign firms? R&D spending as a share of total R&D spending in the U.S. has also slightly declined since 2000.

We need more foreign investment, not less.

In some cases—a very narrow set of circumstances—foreign investment does raise real national security issues. In those cases, the CFIUS process works, and works well. Through hearings like this, Madam Chairman, I am hopeful that the Congress will have additional confidence in the integrity of the CFIUS process. And with good legislation, the business uncertainty that has come in the wake of Dubai Ports will be reduced or eliminated, facilitating enhanced investments, new jobs and more economic activity in the United States.

Thank you for the opportunity to testify before your committee.

Ms. JACKSON LEE. I thank the gentleman. We allowed you to pontificate a little bit longer, and we thank you for your expressions.

Let me thank the witnesses for their testimony—I thank them for statements that open the door. And we are here to do some fact-finding. We are not here to prejudge or presuppose, and there are members on the committee who, I know, would have differing opinions.

And let me indicate that we are going to move quickly. I understand there are certain flight obligations, and I understand also that we are in between and betwixt activities on the floor.

But let me then pose a question in the context, as quickly as I can, to indicate that we have a no—if you will, an environment that we are in now, Mr. Garcia, Mr. Pfister, Mr. Marchick, that is stable and steady; and your testimony suggests somewhat that all is well.

And I started out by indicating that we don't deal with the wellness of security; we deal with the fractures and the possibility of fractures. And I think we have made it very clear that we are not interested in violating or at least undermining the free flow of the economy.

Frankly, another viable hearing would be the question of China's dominance, and I know that Financial Services has probably engaged in that in terms of the sizable investment that they have here in the United States, particularly in the financial institutions. That is not this committee's jurisdiction per se unless we discuss issues involving critical infrastructure. But these are very large questions that have to be asked and answered, so I hope the witnesses will answer my questions in the context that this is not an indictment of the witnesses as much as it is a fact-finding effort.

And I will start first with Mr. Garcia.

I have had the pleasure of working with Mr. Garcia in working with the management and leadership of the FBI. So I imagine you have a fuller understanding, and I would like you to—and I hope Shell will give you that latitude—to broaden your answers and how it relates really to, your background in the FBI.

Just to lay the groundwork, we know that you stated in your testimony that one-third of Shell's assets and shareholders are in the U.S., thereby implying that two-thirds of your assets and shareholders are foreign. In addition to being a foreign-owned company,

Shell is global, which operates in more than 130 companies and employs 108,000 people. And I would assume some of them are foreign nationals worldwide.

Would you please elaborate on the specific additional security measures you take, both in terms of physical security over critical infrastructure and data security over information, because Shell is both foreign owned and a global company.

And may I ask this question right here before so that we can separate some of the issues that you will be answering as it relates to Shell?

But the foreign ownership and foreign investment issue sometimes relates to countries whose relationships with the United States are not as long-standing as those that we have with the Netherlands. Would you agree to that?

Mr. GARCIA. That is correct.

Ms. JACKSON LEE. Therefore, when you raise these questions, when our committee raises these questions, we are not just necessarily thinking that Shell has to be before us as a witness, but we have to address it as it relates to investments that may come from countries who have a short-term friendship with us versus a long-term.

And if I can yield to you now for a response to my question on the security measures.

Mr. GARCIA. Thank you.

When I retired from the FBI and took employment with Shell security, Shell security at that time was addressing all of the issues since 9/11, addressing all of the regulatory issues and regulatory information that was coming from Congress and other governments to the U.S. for protection of infrastructure.

When I came on board, the position that I took, it was brand new; it had not been there before. And the purpose of that, my position in coming in there, was to look at the United States infrastructure, look at how Shell is operating in order to do what you are asking about: protection of the infrastructure, protection of the critical assets that are here and then how we interact with the rest of our partners around the world, the two-thirds, as you mentioned there.

We have very strict procedures on how we deal with information, how we deal with information-sharing between agencies in the U.S. Government, information we share with our expats or foreign nationals that work with Shell.

All of our facilities are controlled. All of our facilities, as far as the people that are there, we know who they are, we have background on them. We have no—we know exactly the access that they have, and one facility in the U.S. cannot be accessed by another person, even by a U.S. person unless they have authorization, escorted if they do not have authorization to be there on their own, or for what type of reason they are going to be there.

The information we receive from these different things, we look at it, we vet it, and we keep it within the close realm of the security group.

And also maintained in its information in a classified type of PKI encrypted system to where—and we only have access—that is not just open to the Shell Group in the U.S. or even overseas. We try

to maintain these proper controls and limit what the information is so that, therefore, it does not get into the wrong hands. Only authorized personnel have access to this information, and that is only a handful of people and, some places, dependent on what exactly the information is.

Ms. JACKSON LEE. Is everyone carded and everyone vetted around your critical infrastructure in places other than the United States and in the United States?

Mr. GARCIA. That is correct. In those facilities they have credentialing that goes into facilities there. I, myself, cannot go to another foreign country, go into a facility and just walk in; they cannot do it in our facility.

Ms. JACKSON LEE. You might recall when Russia froze its gas exports into Europe, the critical impact that occurred. Would you imagine the possibility, the way you are structured now, that happening by an individual act of an employee? Because we have established that, at this point, our relationship with the Netherlands is certainly a, collaborative, cooperative relationship. But would you envision—or would you have the ability if that was an individual act of an employee or set of employees?

Mr. GARCIA. The possibility to have it happen here in the United States is slim. To have one employee just turn off a particular major gas line takes more than just an individual doing that. There are checks and balances that are established that I am aware of, from the process at the refineries; and the gas plants have some type of deviation from that. There is a work blot-out; those who work are advised as—security, as well—to make a determination as to what is going on here.

Nothing is 100 percent. You always have that lone wolf. You always have that individual who can do something on their own because you cannot be in the minds of everybody. But the procedures and the checks and balances that they have in each facility and how they do things help to try to mitigate that.

Ms. JACKSON LEE. Thank you.

Mr. Pfister, let me raise the question of access and control. And thank you very much for focusing most of your testimony on technology. But let us go back to the question of Dubai and the relocation or joint location, if you will, of corporate headquarters.

As I understand, it is being reinterpreted to being jointly—two joint locations, Houston and Dubai. But in the course of your leadership, being in Dubai would suggest that there would be lead space. There would also be the appropriate resources for the joint corporate office to function.

What procedures do you have in place that would give us comfort that any actions in Dubai by anyone who would be in that particular area would not have access to critical infrastructure that could impact America?

Mr. PFISTER. Thank you for giving me the chance to clear that up because there was a lot of misperception around that.

We didn't plan on moving the company to Dubai. We are a proud American company, incorporated here since—

Ms. JACKSON LEE. I am glad to allow you to restate that again.

Mr. PFISTER. The reality—the way the IT security environment works is that, for decades, key employees have been moving all

over the world and where they move and where they office and where they sit doesn't necessarily mean that the information that they need to have access to sits in that same location. In fact, it is much more likely for you to have your key information, your critical information, to be stored in data centers that have been physically secured in locations. You are comfortable around the environmentals, you are comfortable around access, you are comfortable about the security that you can put around that. And, in fact, that is the case in our computing environment. We take very good care of all of our digital crown jewels, and we put them in places where we have the fullest confidence that they will be well protected and access will be controlled.

Ms. JACKSON LEE. Would some of those be housed in the offices in Dubai?

Mr. PFISTER. Very few. Our particular security model is to put as little technology as possible in those locations.

Generally we will put in, obviously, end-user devices such as PCs and laptops, and then we will put in local networks to allow them to talk to each other; but very seldom in other locations, other than our major data centers, which for us today, in an HP-managed facility in Toronto, in a Halliburton-managed facility in Houston. Very seldom do we push anything more complex than that.

Ms. JACKSON LEE. I will raise some more questions with you later.

Mr. Marchick, your testimony focused on the value of investment, and I don't think we have a disagreement in that. But I did note that you gave short shrift to the concept of the purchase, or the proliferation of the purchase of roads, toll roads, et cetera, noticing that this had been a phenomenon in Europe for a long time. However, the framework of this hearing is we must think of what could happen.

Do you still want to give short shrift to the idea of loss of access and control or the interest that should be established as to have certain markers, certain criteria, certain oversight in terms of making sure that during a time of crisis, man-made disaster or natural disaster, that the people of the United States have access to these facilities or to these roads?

Mr. MARCHICK. Madam Chairwoman, the first thing I want to do is learn the critical lesson in Washington: Never disagree with the Chairwoman.

Ms. JACKSON LEE. We welcome your opinion.

Mr. MARCHICK. My view is that the government has a responsibility to ensure that security is in place whether it is a U.S. or a foreign investor, a U.S. or a foreign owner. And with a toll road, that starts with the regulatory structure that is in place or the structure that is in place for that asset.

So, for example, if there are concerns about access to a road in a time of emergency, there should be provisions in place so that either the owner follows instructions of the government in times of emergency or the government gets out of the way and the State, local, Federal Government can take over the entrance and exits to a toll road at a time of emergency; but that the government should only intervene if there is a marginal increase in the risk as associated with a foreign investment.

And with a toll road, I frankly think it is hard to see how a foreign investor could have a negative impact on a road. I think there is a very legitimate policy debate, which I want to stay out of, about whether roads should be privatized or not. But whether it is owned by a Canadian company or a U.S. company, or an Australian company or a U.S. company, I am not sure makes that big of a difference. If it does, the government should intervene and put security measures in place.

Ms. JACKSON LEE. Let me yield to the distinguished gentleman from California for 5µminutes.

Mr. LUNGREN. Mr. Garcia, when were you with the FBI in L.A.?

Mr. GARCIA. June of 2001 was when I first arrived there as a special agent in charge, and I lived in Long Beach. Not to mention that—

Mr. LUNGREN. You obviously have good judgment. I appreciate that.

Ms. JACKSON LEE. I won't take from your time, Mr. Lungren, but he is now back in Houston, and he started in Houston.

Mr. LUNGREN. I know. I understand.

Mr. GARCIA. I am a Texan.

Mr. LUNGREN. I understand that. You miss the humidity and the sweat. I understand that.

In your testimony, you note that Shell participates in the Homeland Security Information Network and Homeport. Is there any difference that you can ascertain between the cooperation and the relationship you have with the Department of Homeland Security here as opposed to if you were not a subsidiary of a foreign-owned corporation?

Mr. GARCIA. If I understand your question: If we were a foreign corporation strictly, not have U.S. ties, as Shell has here in the United States, would there be any difference on how DHS works with you? I would imagine that DHS is limited on what they can share with anybody, depending on their nationality, depending on the information that they have and that they are actually trying to put out.

Mr. LUNGREN. But as a wholly owned subsidiary of a corporation, do you have any—

Mr. GARCIA. We have no restrictions whatsoever on how they deal with us because of the fact that we are U.S. persons, too.

Mr. LUNGREN. Mr. Pfister, could you clear up for me, I don't understand this idea of dual corporate structure Dubai, Houston. What is—what do you have in Houston and what do you have in Dubai in terms of corporate headquarters?

Mr. PFISTER. Well, Houston is our principal place of business. It is where we have the majority of our corporate officers; it is where we conduct the majority of the strategy settings and the design making of our company. So it is our corporate headquarters.

Mr. LUNGREN. What is Dubai?

Mr. PFISTER. Dubai is going to be the location of our chairman and chief executive officer. It is our opinion that it is in the best interest of the country for Halliburton to be as strong in the energy business, and in order for us to do that, we have to be as strong in the Eastern Hemisphere. You have probably seen some of the

statistics that are there; 60 percent of the oil reserves are in the Eastern Hemisphere, so he is moving over to Dubai.

We will probably consolidate some of the other managers that are in that general region, and that will be his base.

Mr. LUNGREN. So you have got more business over there than you have here?

Mr. PFISTER. No, that is not the case now. We conduct well into the majority of our business in North America today, but we need more valuable portfolios because that is where most of the reserves are.

Mr. LUNGREN. And reserves you can go after, I presume.

Mr. PFISTER. Yes.

Mr. LUNGREN. Last time I checked, you can't go offshore, Florida, California, offshore in the eastern part of the United States. You can't go in ANWR. Am I right in those things?

Mr. PFISTER. It is better probably to ask our Shell representative, because we don't get involved in this debate, but I think it is accurate.

Mr. LUNGREN. I can't understand why you would move to where the business is. That is just bothersome.

No. I mean, you know, we have made it almost impossible for us to go after new resources in the United States in our environs, and I always remember the people who used to drive to the protests against offshore drilling in California. Very few of them came there via skateboard or walking. I guess it was magically produced for them.

That is just a little thing I have. I mean, I grew up in Long Beach, as you know, and Long Beach, we have manmade oil islands. We have 2 billion proven reserves. We actually do slant drilling there. We had the first, the beginnings of injection wells for the purpose of boosting the city back up, and then we got into the whole idea of using it for secondary and tertiary recovery.

We are looking at the Signal Hill reserve, which I think is the fourth oldest continuous operating reserve in the country, and we actually have potential for opening up wells there because we put more money into it. It is kind of interesting. A lot of people get in their car and figure that comes there.

Anyway, Mr. Marchick, you were talking about the CFIUS process and the ambiguity in which infrastructure will have an impact on national security, complicating foreign investment. We in the Congress responded to a concern that was expressed that we needed to bring CFIUS up to date. One of the concerns I had as we did that was, we should—would we be bringing too many transactions within that ambit? Would that cause us to spend too much time and attention and have our intelligence communities focusing across the board on what would end up being nonimportant issues, and therefore, not being able to give the appropriate analysis to those which truly had a national security interest within what we know have to be some sort of reasonable time limits; otherwise, you are not going to have the investment because we make it impossible.

How do you suggest we balance that? You talk about ambiguity, which means you think we ought to have more particularity. What kind of particularity would you talk about?

Mr. MARCHICK. The first thing to do is define what critical infrastructure is for the purposes of foreign investments.

As I mentioned, during the Clinton administration there were eight sectors defined as critical infrastructures. Now there are 12, but there have been four different reports in the last 4 years that define it differently and give different sectors. That is all for the purpose of physical protection of critical infrastructure.

Take a stadium, for example. You want to protect that from being blown up or from some tragic circumstance, but who owns a stadium, you know, doesn't have any impact on security. So I think the most important thing to do——

Mr. LUNGREN. You obviously haven't been involved in the debate on building a stadium in DC.

Mr. MARCHICK. Building or not building is a key issue, but who owns it doesn't raise any security issues.

The key issue is for the government to provide guidance on what they mean by critical infrastructure for the purposes of foreign investment. They define agriculture as critical infrastructure. Who owns a farm, whether it is owned by a Canadian or an American, I can't see the difference from a security perspective.

So in the Senate bill that passed the Senate today, the Senate Banking Committee, there is a requirement for the CFIUS agencies to provide guidance to the investment communities on the type of transactions they are seeing. That would be very helpful. Because right now there is a lot of ambiguity, and you are forcing a lot of transactions into the CFIUS process that don't need to be there. And you are requiring the intelligence community, the Homeland Security Department and others to spend a lot of time on those when they should be focused on the transactions that really matter.

Ms. JACKSON LEE. Thank you.

The gentleman's time has expired.

It is my pleasure to yield to the distinguished gentlelady from New York, Brooklyn, New York for her 5 minutes.

Ms. CLARKE. Thank you, Madam Chair.

It has been somewhat of a hectic day today, but I thought it was very important to be at this subcommittee hearing. I just want to share a couple of thoughts and raise a couple of questions.

Since the very beginning, foreign investment has played a vital role in the development of the United States; as the world becomes increasingly global and the businesses around the world find new ways to integrate, maintaining a strong level of foreign investment will be as important as ever.

There is also a great deal that foreign companies can't do to keep America secure. By working with the government and reducing their vulnerabilities, companies can both improve the economy and help maintain security. This, however, is dependent on a strong, cooperative relationship with the government and on maintaining sensitive information and systems in a safe way.

We must also keep in mind that not all investors have the best interest of the U.S. at heart. Therefore, the government must continue to play a role in determining which investments could cause harm to come to Americans.

I wanted to direct my question to you, Mr. Pfister. How exactly would you define critical infrastructure? That has been a lot of the

challenge. You know, I come from New York State where, of course, the big issue around Dubai Ports became a national issue and national concern. And I think defining critical infrastructure and what it means in this global environment that we are in, is really important.

Because I notice that you comment in your testimony that Halliburton does not possess any critical infrastructure or assets, I want to know whether you would consider various energy facilities—you operate critical infrastructure; or what about operations which involve supplying or building facilities for our military overseas?

Can you just sort of give me a sense?

Mr. PFISTER. Yes, ma'am. I would be happy to do that. Let me kind of start off—all right. Is it better now? This must be the microphone. I would be happy to answer those questions.

Let me explain kind of what our assets are that we do own. We own people, obviously, with intellectual property between their ears. We have got manufacturing plants all over the world that build equipment, heavy equipment and tools that are mobile enough to then drop-ship into different parts of the world, so the big trucks and the skids and the boats that go out and provide services in the more permanent critical infrastructure that Homeland Security has appeared to focus more attention on in the past.

We have technology centers where we do—we have laboratories where we do research and development of our products. And then again, we have the equipment, the actual equipment.

So when we made the statement up at the—in my opening statement that we were really not the owners or the operators of critical infrastructure, we were using the more classical definition that Homeland Security has had of refineries, pipelines, LNG terminals, et cetera. We don't operate or own any of those.

What we operate and own are tools that fit in trucks that we drive around or we float to different locations to actually help us.

And the complexity around them is that our primary technology is in better understanding rock properties and fluid properties, deep underground, and figuring out how to make hydrocarbons flow faster out of that and get to the surface. So our equipment is very specific, very niche-oriented to that.

So I don't know if that answers your question or not.

Ms. CLARKE. It does to a certain degree. But being an avid watcher of the television program 24, I will submit to you that the tools that you utilize getting into the wrong hands or being exposed to the wrong environment could pose a threat. Just FYI

Let me follow up with this question: If Halliburton's operations were run by an entity that wished to do harm to America or shift U.S. policy, do you feel they would have a means through your operations to accomplish this?

Mr. PFISTER. Can you clear up the question just a little bit? If Halliburton's operations were bought by someone else and then controlled?

Ms. CLARKE. By that entity.

Mr. PFISTER. Well, it wouldn't be too different than some of our competitors today. Schlumberger is not an American corporation and yet we allow them to operate in the United States and in other places around the world.

I guess you are asking me for my advice on whether foreign ownership of the sort of business that we operate today would create any incremental concerns.

Ms. CLARKE. Vulnerabilities.

Mr. PFISTER. I have a hard time seeing that being a large increase in risk.

Ms. CLARKE. OK.

Mr. MARCHICK. I would just note, it was the microphone of the foreign company that didn't work.

Ms. CLARKE. That is a good one.

Mr. Marchick, in your testimony, you express several definitions for critical infrastructure. Which do you feel is most appropriate, or do you have a separate definition you feel would better fit?

Mr. MARCHICK. I think the definition in the PATRIOT Act is a very good definition because it focuses on those systems and assets whose destruction would have a debilitating impact on the United States.

We know that, for example, in some sectors there is an incremental risk in foreign investment. For example, in the telecom sector because the Department of Justice wants to have access to wiretaps that we want—they have a legitimate interest in ensuring that they can conduct those wiretaps without foreign persons knowing about them or without foreign governments knowing about them, so you want to have American citizens handling those wiretap processes.

Similarly, you want American citizens handling classified information in defense companies.

But I think there is a very narrowly defined set of sectors where there really is an incremental risk for foreign investments, and in most of those sectors, if not all of them, there are ways to mitigate that risk through, for example, requiring that American citizens operate in key functions at a port facility or in a telecommunications control center or in the defense sector by making sure that all of the people that have access to sensitive assets have background checks and security screens, and there are access controls and badging and escorts.

So I think that we shouldn't seek to ban foreign investment. We should seek to mitigate the marginal increase in risk associated with foreign ownership in those very narrow sets of sectors where foreign ownership matters.

Ms. CLARKE. Just to follow up, Madam Chair.

Mr. Marchick, in your experience, do you feel that CFIUS takes into account the country in which the potential foreign owners are based? Does it treat various countries differently, and are you aware of any situations where CFIUS denied a filing purely on the nationality of the company?

Mr. MARCHICK. CFIUS looks at a variety of factors in their national security analysis. They start with looking at the threat and whether there—if the buyer had harmful intent and the capability, would they do something to harm the interest of the United States.

They would then look at the vulnerability. What are the assets that the company is buying and how could a person or entity that has the intent to harm the United States take action to harm the United States?

The country where the buyer comes from is a factor. British companies are treated differently than companies from other countries. Privately owned companies are treated differently than government-owned companies. And the ownership does have a significant impact on the national security risk analysis that the CFIUS agencies undertake.

I am not aware of any specific ban outside of existing law on companies from certain countries investing in the United States, but I do know that certain countries that make investments in the United States have higher scrutiny than others.

Ms. CLARKE. Thank you very much, Madam Chair.

I yield back the rest of my time.

Ms. JACKSON LEE. I thank you.

I am aware of your schedule. We will be back before that time. And we will recess for the last time. When we come back, we will conclude the hearing.

[Recess.]

Ms. JACKSON LEE. The subcommittee hearing is called to order. Thank you so very much for your patience. I know it will add to your happenings here on the Hill.

Let me first, in the absence of my ranking member—I know that he has been called to another hearing which I am called to, so we will finish at this time. Just—in his absence, as well, I will make sure that he knows that he has a few friends in Texas who believe in the energy industry and the value and importance that it has for the United States.

With that in mind, Mr. Garcia, let me just quickly get a quick question to you. Plain and simple, how are these lessons applied to assets that are or affect critical infrastructure in the United States?

The lessons that we are talking about, of course, are the fact that you are a global company. If you could, just restate for us how the lessons of being global can impact on the securing of assets here in the United States which happen to be under the control of foreign investors.

Mr. GARCIA. Since 9/11, the United States has really tightened its security measures on all aspects of life here. Everybody is more conscious of what is going on—law enforcement as well as companies, if they can take stringent measures to try to protect against another attack since 9/11.

For attacks that take place overseas, we are in countries where security measures are not as strict as in the United States. The insurgents in Iraq and places in other locations, we see what they do. We learn from what they are trying to do and how to do it, and see what we can do to ensure that that does not happen here in the United States.

We take those lessons learned by looking at and studying what they do to ensure that we are covering our procedures, that we have to plug that gap. We always try to look at the "what ifs," as you suggested earlier. We do not just take things for granted. Anything can possibly happen, so we always look at the impossible and say, "Do we have a coverage for that or not?" Using the overseas incidents that take place, we look at that as well.

Ms. JACKSON LEE. Mr. Marchick, let me just, as we excuse you and thank you for your testimony, raise this last question with you.

I, frankly, believe that we need legislation that is geared toward the question of actual security of the infrastructure, of the critical infrastructure; and certainly CFIUS has a lot of elements in it. I will certainly be looking very closely at the markup that the Senate has done today.

Give us, if you will again, your parameters or where you believe there should be government intervention, and we hope that you will not be inhibited by your clients. We are asking for your wisdom and so—frankly, I think you started out by saying, where there was a crisis or where there shows to be some inconsistency or problems, there might be a need for government intervention. Would you expand on that, please?

Mr. MARCHICK. Thank you very much.

Let me just state for the record that these are my opinions. My clients have opinions all over the map, and hopefully, I will not get fired by any of them after what I say today.

It seems to me that the Federal Government, working with industry, should develop security guidelines, security mechanisms, security standards on a sector-by-sector basis, addressing the risk that is inherent in that sector.

The Department of Homeland Security is doing that now in the chemical sector, coming up with chemical security guidelines and chemical security regulations, working with industry. That is a very healthy exercise.

On top of that, if there are marginal increases in risk to our national security associated with foreign investment, those should be addressed through CFIUS; and CFIUS, I think, is well-equipped to address those particular concerns, but it is that marginal increase, that delta in security risk that is the only thing that CFIUS should focus on.

The general vulnerabilities that exist in our energy sector, for example, or our chemical sector should be addressed across the board regardless of who owns the asset. And then on top of that, if there are particular issues associated with a particular foreign owner who raises issues, those should be addressed through CFIUS. And I think that this committee and the CFIUS committee and the Homeland Security Department can work together to accomplish those twin goals.

Ms. JACKSON LEE. So, if you will, as to an established conflict that may generate between the United States and another sovereign nation that might interfere with critical assets or with that country's investment in the United States, you are suggesting that that should be looked at isolated or it should be looked at separately?

Mr. MARCHICK. I think it should be looked at with great rigor to see if there are risks that a foreign owner would do anything that would harm the security of the United States. And we should never allow that to happen, but we should start by ensuring that we have strong security measures in place across the board; then—going back to the security philosophy that Mr. Pfister and Mr. Garcia articulated—have a layered approach, have additional security condi-

tions to address particular concerns that are associated with a foreign investment.

So you start with a basic building block of security for our critical infrastructure, and if there are additional risks associated with foreign investors, CFIUS should impose conditions on that transaction to make sure that those security issues are addressed.

Ms. JACKSON LEE. So you add to CFIUS or you may look also at a more narrow focus on homeland security?

Mr. MARCHICK. Exactly.

Ms. JACKSON LEE. Let me thank you, Mr. Marchick. I understand you have a flight.

Let me conclude with Mr. Pfister.

Let us try to probe again, just as we close this hearing, to have a better understanding, because Dubai has created a great deal of interest, and the presence of your CEO and other personnel have created a great deal of interest. That, in essence, Mr. Pfister, is an investment of sorts.

I assume that you are leasing property or buying a building. You are possibly having access and control. So our inquiry is equally, certainly for the safety of the personnel and for the safety of whatever resources you utilize.

Can you again frame for us how you provide the protection of any critical infrastructure that might be necessary to ensure your work in Dubai or in Doha or wherever you might happen to be?

Mr. PFISTER. Yes, ma'am, I would be happy to.

To be quite frank with you, Dubai is one of the easier places to secure and protect infrastructure, particularly of the information technology. They are one of the more advanced countries around the world in terms of providing capabilities and digital technologies, once you have figured out how to provide acceptable security in places like Africa and other places—in Russia, Falkland Islands, and other places that the energy industry operates.

Ms. JACKSON LEE. So how do you proceed in those difficult areas?

Mr. PFISTER. So it is using the standards.

One of the phenomena around information technology security is that security improvements are cumulative. The financial industry creates new ways of protecting financial data, and it immediately becomes available in commercial products that then other industries are able to deploy. The health care industry creates new technology approaches and commercial products that we then embed in other industries. So, you know, this is not a brand-new phenomenon.

With the advent of the Internet and when companies started hooking their computer networks up to, you know, the globe, that risk was introduced at that point in time; and so the commercial IT security industry and companies participating in groups like the API and others have been designing firewall systems, prevention systems, approaches to secure computers and assets that are almost mainstream at this point in time.

So Mr. Lesar's move to Dubai really does not materially increase at all the risk that any of our key technologies or our key intellectual property is going to be exposed to, any more than it was in the last decade as we have had people traveling all over the world, many times much more and to more desolate places than Dubai.

Ms. JACKSON LEE. Do you have enhanced security measures of personnel? Do you have reinforced buildings? Do you do anything differently?

Mr. PFISTER. Well, we do the same types of security, from the physical security aspects, that you heard about from our Shell associate: guards; you know, big cement blocks as you enter the building so that car bombs and things like that would not get into the core of the building; the same card key access; the same logging; those types of things. So it is really not any different than the way we protect any other location that has computers that might have access to critical information.

Ms. JACKSON LEE. Let me say that I think the test may be the word "rigor" in that we should be rigorous when we are looking at foreign ownership and foreign investors as it relates to our security.

My last question to you, Mr. Garcia, is that—again, using your expertise—we do know that oil companies—many of them are in and invest in continents—South America, the continent of Africa. We know in particular that there has been some well-known publicized seizing of assets in the delta of Nigeria. That obviously has a life of its own, but I want to pose a question which is similar to the Russian incident that occurred that impacted Europe.

If the resources were stymied such that there would be the foreign investment by a foreign company but they would be impacting the UnitedμStates, what kind of intervention are you all looking toward to prevent that kind of major impact? Even though resources go all over the world, what are you looking toward to prevent that kind of major impact on energy resources coming to the United States?

Mr. GARCIA. Congresswoman, the actual dynamics of the oil flow's being cut off in various countries outside the United States would probably be answered best by somebody in the company that deals with that.

As far as the security issues there in Nigeria, I monitor that with the Shell security group to see what measures can be done and to see what assistance can be provided to them either through the host country or through other types of training and activities that can be done with the various U.S. embassy personnel who are there, to help alleviate some of those problems and some of those issues so that we do not get to this position where it is not safe to do any business at all in that particular country.

As far as the impact, I would imagine the impact of cutting off any kind of reserves coming to the United States can be detrimental to the United States economy depending on how much is cut. As far as how and specifically what the impact would be, some other witness will probably have to answer that on the economics part.

Ms. JACKSON LEE. Do you think, in the whole idea of security and critical infrastructure around the world, that the Federal Government, beyond the existing legislation, can be more helpful?

Mr. GARCIA. Well, the Federal Government right now is working a lot with the Coast Guard on the international port security program where they actually go to the various ports around the world that service ships that come to the United States—our tankers and

other things that do come here. They are doing a big push in working with the various countries that these vehicles or vessels come from in order to try to ensure that the security measures that are taken on in those host ports overseas are helpful for what is coming to the United States.

Some of the exceptions that are done are that the Coast Guard will do inspections and boardings offshore well within the safety region away from the United States so as to ensure that the vessel itself is not something that is going to be detrimental or dangerous to the United States when it comes to our ports.

So the United States and the Federal Government are doing a lot of things overseas to help in that aspect, and we, as an industry, are trying to assist them on identifying weaknesses and vulnerabilities that they should be looking at and are trying to ensure that they search and look at those areas to try to prevent some sort of an act.

Ms. JACKSON LEE. Let me conclude and thank you very much for the response.

Just in summary, this has been a challenging time to have a hearing, but I thank you for giving us at least the beginnings of our discussion on this issue. As I indicated, I think there is more to explore. This hearing was to begin the discussion, as we have started under the full committee with ChairmanµThompson.

How do you protect foreign infrastructure that may be in the hands of a foreign owner that impacts the United States, our national security or a foreign investor? There are a lot of nuances that will take several panels and very long hours, but I will end as I started.

Our challenge is to imagine the possible and the impossible, and it is also to accept the premise of our economy, which is an economy that welcomes investors, but at the same time, as for the persons who we have the responsibility of protecting, we have to ask the hard questions.

So I believe that we have been given, even from your testimony, a range of issues to think about and a range of issues to look at—expanded legislation—in light of the long list of critical infrastructure that we have, to be able to at least give guidance to public entities, which are separate from Mr. Garcia and Mr. Pfister.

And also to our corporate entities, which already probably have a major leg forward, because statistics show that you have about 85 percent of our critical infrastructure, both domestically and then those that are owned by foreign investors that are in the private sector; and you certainly have concern about your own property and the needs and protection of your own employees.

We know you are forward-thinking, and I think it is crucial that we take up the responsibility for those issues that may not be as far ahead as the private sector is, and I count that as the raging new, if you will, basis of securing funding for public entities, and that is the selling of the very roads upon which we travel. That is a major issue, and I think that we should certainly look at that.

You have given us a great deal of insight. We thank you for your appearance here before our committee, and I believe that I will follow up with my concluding remarks so that we can finish.

As I have indicated, I thank the witnesses for their very valuable testimony, and the members of the subcommittee may have additional questions for the witnesses, and we will ask you to respond expeditiously in writing to those questions, and we will look forward to the answers in the response.

Ms. JACKSON LEE. I am going to put into the record, with the existing quorum, an article by a Times reporter in Philadelphia, "Foreign Companies Buying American Roads and Bridges"—it happens to be a positive article—and an article from the Dallas Morning News, "Foreign Companies Buying U.S. Roads and Bridges." Those are some of the other aspects of the work that we have before us in this committee.

So let me thank all of the witnesses. With that, the hearing is adjourned.

[Whereupon, at 5 p.m., the subcommittee was adjourned, subject to the call of the Chair.]

○

VerDate Nov 24 2008 08:36 Jun 25, 2009 Jkt 000000 PO 00000 Frm 00039 Fmt 6633 Sfmt 6011 H:\DOCS\110-HRGS\110-36\48911.TXT HSEC PsN: DIANE