AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

FOREIGN OWNERSHIP:

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

MARCH 23, 2007

Serial No. 110–21

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

43–557 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

VerDate Nov 24 2008 09:10 Jun 08, 2009 Jkt 000000 PO 00000 Frm 00001 Fmt 5011 Sfmt 5011 H:\DOCS\110-HRGS\110-21\43557.TXT HSEC PsN: DIANE

Congress.#13

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*
TODD GEE, *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)*

D. MICHAEL STROUD, *Director & Counsel*
NATALIE NIXON, *Deputy Chief Clerk*
COLEY O'BRIEN, *Minority Senior Counsel*

VerDate Nov 24 2008 09:10 Jun 08, 2009 Jkt 000000 PO 00000 Frm 00002 Fmt 0486 Sfmt 0486 H:\DOCS\110-HRGS\110-21\43557.TXT HSEC PsN: DIANE

CONTENTS

Page

STATEMENTS

The Honorable Sheila Jackson Lee, a Representative in Congress from the State of Texas, and Chairman, Subcommittee on Transportation Security and Infrastructure Protection 1
The Honorable Daniel E. Lungren, a Representative in Congress from the State California, and Ranking Member, Subcommittee on transportation Security and Infrastructure Protection 3
The Honorable Gus Bilirakis, a Representative in Congress from the State of Florida 29
The Honorable Yvette D. Clarke, a Representative in Congress from the State of New York 27
The Honorable Eleanor Holmes Norton, a Delegate in Congress From the District of Columbia 30

WITNESSES

The Honorable Stewart A. Baker, Assistant Secretary for Policy, Department of Homeland Security:
Oral Statement 6
Prepared Statement 10
Ms. Ann Calvaresi Barr, Director of Acquisition and Sourcing, Management Government Accountability Office:
Oral Statement 14
Prepared Statement 16
The Honorable Gregory Garcia, Assistant Secretary for Cybersecurity and Telecommunications Department of Homeland Security:
Oral Statement 10
Prepared Statement 14
Colonel Robert B. Stephan, Assistant Secretary for Infrastructure Protection, Department of Homeland Security:
Oral Statement 8
Prepared Statement 13

VerDate Nov 24 2008 09:10 Jun 08, 2009 Jkt 000000 PO 00000 Frm 00003 Fmt 5904 Sfmt 5904 H:\DOCS\110-HRGS\110-21\43557.TXT HSEC PsN: DIANE

DISCUSSION OF CHALLENGES POSED BY FOREIGN OWNERSHIP TO USING CRITICAL INFRASTRUCTURE

Friday, March 23, 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 10:08 a.m., in Room 311, Cannon House Office Building, Hon. Sheila Jackson Lee [chairwoman of the subcommittee] presiding.

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

Ms. JACKSON LEE. [Presiding.] Good morning. The subcommittee will come to order.

The subcommittee is meeting today to receive testimony on challenges posed by foreign ownership to using critical infrastructure and how the Department of Homeland Security is working to protect critical infrastructure.

The chair wants to acknowledge the presence of the ranking member, Mr. Lungren of California, wants to acknowledge the presence of Ms. Clarke of Brooklyn, New York, and the presence of Mr. DeFazio of Oregon.

I have often indicated that, as I have served on this committee, the Homeland Security Committee, and seen a number of individuals who come before us with the responsibility of securing the homeland, that we live in a new climate and a new era after 9/11. In fact, this committee and the department was not a fixture of government prior to 9/11.

That poses an enormously heavy burden and responsibility, one that I believe all of us accept. But what it does say is that unlike our committees of jurisdiction, that if a tragic and horrific act were to occur again, that America would look to all of us.

I believe Chairman Thompson, and certainly I agree with him and will continue to work with that mission and message that we have to be continuously subjective and objective in looking at the responsibilities of the elements that make us secure.

Critical infrastructure, in this instance, has a vast landscape and this committee is committed to reviewing the aspects of critical infrastructures in the United States and as relates internationally, as it may impact on the securing of America.

VerDate Nov 24 2008 09:10 Jun 08, 2009 Jkt 000000 PO 00000 Frm 00005 Fmt 6633 Sfmt 6633 H:\DOCS\110-HRGS\110-21\43557.TXT HSEC PsN: DIANE

I would then like to take the opportunity to thank all of us and all of you for joining us this morning so that we can begin our exploration of the topic of foreign ownership and how it intersects with national security.

A little over a year ago, Congress united to oppose the administration's failure to conduct an adequate oversight when there was a proposal by Dubai Port World to enter into a deal that would have put Dubai Port in charge of managing many of our USC ports.

The issue became a particular concern not because Dubai Ports was a foreign company, but because it was one that was controlled by a foreign government.

Needless to say, I believe most members will say to you that we understand internationalism and trade and opportunity and exchange, but it is important for all sovereign governments to protect the people which they have responsibility for.

On the heels of September 11, this deal raised well-deserved skepticism of how the United States monitors and evaluates foreign ownership of our critical infrastructure. Today, more than a year later, we continue to monitor this issue closely by holding this hearing and others that will explore the Department of Homeland Security's involvement with the Committee on Foreign Investment in the United States, CFIUS, as some would call it.

Before 9/11, the process was not a strong focus of many Americans. As we know, this country relies on foreign investment. As a recent Congressional Research Service publication indicates, foreign investment in the United States could top $160 billion for 2006. Thus, while foreign investment is a great resource and indicator of our strength in the global economy, we must be vigilant that we do not compromise security.

After 9/11, our outlook on foreign investment and especially ownership of critical infrastructure changed. Americans, including myself, began to wonder who is watching foreign investment is being made in the United States, where is it being made, and how vigilant are we being in making sure that the elements that they may possess that relate to America's security are, in fact, protected.

There are many more questions that we might ask. One of them being the process that is used by CFIUS whether or not, even with the presence of the secretary of homeland security on the committee and involved in the process, what strictures have we put in place, what regulations, what directions have we put in place to ensure that we are an active participant in protecting America.

I, like most Americans, wholeheartedly support capitalism and, of course, a balanced trade process. Yet, as events have shown, we need to pursue a vigorous oversight agenda, especially in the area of foreign investment in critical infrastructure.

Dubai Ports told us that we need not just focus on in one area of infrastructure, but we need to focus on all areas.

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 its viability here and that it is available when America needs it most, but that it is available by being safe and secure.

As we all know, terrorists don't 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 and attack us with brute force, but simply by pressing a computer button or by crippling a key asset.

It is with this notion that I, along with other members of this subcommittee, am seriously committed to protecting critical infrastructure and understanding how the administration is protecting our vital assets.

One example of how serious we are in taking this role on in this committee is by supporting H.R. 556, Committee on Foreign Investment in the U.S. reform bill. This bill provides needed reform for formalizing and streamlining the structure and duties of the Committee on Foreign Investment in the United States.

I am happy to say that I voted to support this bill, along with more than 400 of my colleagues on both sides of the aisle.

And this bill addresses many of the concerns raised about CFIUS, especially its current lack of transparency and oversight and congressional reporting and accountability.

This bill adds much clarity to a relatively murky process. This bill rectifies concerns from the business community by formally establishing the membership and timelines as to how and when this review would take place.

According to CRS's analysis of H.R. 556, the bill increases the role of congressional oversight by requiring a reporting process on its actions and allowing for a greater amount of detailed information about CFIUS's operations.

But there may be more that we need to do and I believe that there may be legislative need that further enhances our oversight over foreign investment and ownership.

Today we want to continue to explore the role that the Department of Homeland Security has with this new process and how it is accomplishing its goal of overall infrastructure protection.

I look forward to the witnesses' testimony and learning about the process and the department's role that can be fortified, while protecting the United States' interests in international commerce.

It is my pleasure to yield 5 minutes to the distinguished ranking member from California, Mr. Lungren.

Mr. LUNGREN. Thank you very much. I thank the chairwoman of our subcommittee.

And I welcome our guests here who are to speak to us, and I welcome the opportunity to discuss foreign ownership and the challenges it presents for our critical infrastructure.

This Homeland Security Committee is all too familiar with the concerns and fears that foreign ownership of U.S. critical infrastructure assets creates in our citizens.

The purchase last year of the operating rights at six U.S. ports, including the ports of New York, New Jersey and Baltimore, by Dubai Ports World Company created a firestorm of public and congressional opposition.

It also focused attention on the governmental process established to review such sales and determine whether it creates a threat to our economic or national security.

This process of reviewing foreign purchases is done by the now known Committee for Financial Investment in the U.S., or CFIUS.

In 1988, I believe in one of the last things I did as a member of Congress during my first tour of service here, Congress passed the Exxon-Florio provision amid growing concerns over foreign acquisition of American businesses.

This provision gave the president the authority to block proposed foreign acquisitions that were deemed to threaten our national security.

Foreign acquisition of U.S. companies and assets pose a particular challenge to our government. It creates a delicate balancing act in the worldwide economy.

How do we attract vital foreign investment to the United States without sacrificing or diminishing our national security? One of the first questions we have is, what is critical infrastructure? Infrastructure in this country is owned, depending on whose figures you look at, 85 to 90 percent in the private sector, not in the public sector.

So how do we do that? I believe we have the proper procedures to protect our critical infrastructure and assets by requiring foreign acquisitions to be closely reviewed and scrutinized by CFIUS.

For over 30 years, this process has worked effectively, guarding our capital markets, our highly valued infrastructure assets, and, most importantly, our national security.

Most of the time, it doesn't gain any headlines and that was a conscious decision made by the Congress when it set up CFIUS. We did not want to do something that overreached such that we denied ourselves the kind of foreign investment that actually proved to be beneficial to this country. So we set up a process which, by and large, would oftentimes not gain any headlines or public comment.

The problem that occurred last year, however, was there was an area that probably needed some public comment or at least needed to be brought to the attention of the president of the United States and perhaps even to the attention of the Congress before it was made public.

In the years that we have had this law, on only one occasion, in 1990, did the president intervene and order 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 and it demonstrated that changes needed to be made in light of 9/11 and our nation's growing terrorist threat.

Important improvements were included in the legislation we passed last year, H.R. 5337, and, again, in February of this year, H.R. 556, referred to by the chairwoman of this committee, and it did pass by an overwhelming vote of 423–0.

The legislation elevated the secretaries of homeland security and commerce to vice chairs of CFIUS, and I believe it will help address concerns about CFIUS applying too narrow a definition of a national security threat, which was a criticism of past reviews. The legislation also limits delegating these important CFIUS decisions.

I believe the hearing and future hearings will also look into how the Offices of Infrastructure Protection and Cybersecurity and Telecommunications work together to protect key resources, especially as it relates to the CFIUS process.

I would just once again like to say publicly that I appreciate the cooperation and quick response of DHS to a critical vulnerability involving cyber and critical infrastructure uncovered by the private sector, the dispatch with which they dealt with that, the cooperation they showed with this committee, and I look forward to future briefings, particularly of a classified nature, on the success of that overall effort.

And with that, I would yield back the balance of my time and thank the gentlewoman for giving me the time.

Ms. JACKSON LEE. I thank the distinguished ranking member, Mr. Lungren from California, for his statement.

And I would remind other members of the subcommittee that, under the committee rules, opening statements may be submitted for the record.

I welcome all of the panel members this morning and believe that your presence here this morning emphasizes a journey that we will take to expand our oversight over critical infrastructure.

Our goal is to not only reach a point where we believe that we have explored aspects that could be conceived that might harm the United States, but also that we are helping to provide a necessary instructional direction to be able to help to secure these facilities.

Our first witness, Mr. Stuart Baker, who I know has great insight on this issue, is the assistant secretary for policy at the Department of Homeland Security. Prior to joining the department, Mr. Baker was general counsel of the commission on the intelligence capabilities of the United States regarding weapons of mass destruction. And prior to this, he was the general counsel for the National Security Agency.

Welcome, Secretary Baker, and we thank you for your service. We look forward to hearing your testimony.

Our second witness, Colonel Robert Stephan, is the assistant secretary for the Office of Infrastructure Protection with the Department of Homeland Security and was most recently in Houston, Texas.

And I applaud him for that, not only for being in Houston but for also reaching out to constituencies and cities and counties and states in order to get firsthand knowledge. And I think that is extremely important.

Prior to joining the department in 2005, Colonel Stephan was a senior director for critical infrastructure protection in the executive office of the president. Colonel Stephan had a distinguished 24-year career in the United States Air Force.

Welcome, Colonel, and we are happy to have you here, and we thank you for your military service to our country.

Our third witness is Mr. Gregory Garcia. We have had the opportunity to hear the insight of Mr. Garcia previously, and we thank him for his insight. He is the assistant secretary for the Office of Cybersecurity and Telecommunications with the Department of Homeland Security. Prior to joining the department, Mr. Garcia

was the vice president for information security programs and policy with the Information Technology Association of America.

Giving him a balance of both private and public sector, before joining the association, Mr. Garcia worked with the House of Representatives Science Committee, certainly a committee that I have affection for and, as well, a longstanding relationship.

Thank you for coming today. We look forward to your testimony, and we thank you for your service.

Our final witness, Ms. Ann Calvaresi-Barr, is the director for acquisition and sourcing management at the United States Government Accountability Office. Ms. Calvaresi-Barr has been with the GAO for 23 years and is responsible for reporting and testifying before Congress on issues impacting foreign investment, amongst other topics.

We are always appreciative of the objectivity that GAO provides us. We will continue to access the resources, and we hope that you will assist us as we delve into determining how much more work we need to do to secure the homeland as it relates to critical infrastructure.

Thank you for being here today. We look forward to your testimony.

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

I now ask each witness to summarize his or her statement for 5 minutes, beginning with Assistant Secretary Baker.

STATEMENT OF HON. STEWART A. BAKER, ASSISTANT SECRETARY FOR POLICY, DEPARTMENT OF HOMELAND SECURITY

Mr. BAKER. Madam Chairwoman, thank you very much. Ranking Member Lungren, members of the committee, it is a pleasure to be here.

I am very proud of the work that DHS has done in CFIUS. It is the youngest member of CFIUS and I think it is widely recognized as among the most creative users of CFIUS—we are creative because we have to be, because the definition of homeland security requires that we think of a wide variety of risks that other agencies do not have to be concerned with—and as the most thorough member of CFIUS, in many respects, which I will get into.

CFIUS has been around, as the ranking member suggested, for quite some time. It was actually started under an executive order even before the Exxon-Florio Act. We, of course, did not arrive until we were created as a department, but we joined an existing structure that set up a committee of now six departments and a variety of executive agencies, chaired by the Treasury Department.

Our authority is essentially the authority to recommend the president blocking an investment in the United States because of the threat to national security.

In order to determine whether to make a recommendation to block a transaction, we have to do an investigation of our own. The investigation is supposed to last only 30 days. Everyone recognizes that these transactions have short shelf lives and need to be moved forward quickly.

So we have to jump on transactions. It is like being a fireman. As soon as you hear the alarm, you just jump into your boots and get on the pole and go to the fire. And we are doing that more than we have done in years. Filings have gone from about 40 or 50 a few years ago to being on a pace for almost 150 this year.

And we try to handle all those transactions in less than 30 days, if we can. If we can't, if we conclude we need more time, we can ask for more time and we can extend the investigation to 45 more days or ask the parties to withdraw and give us even more time before we have to make a decision.

What do we do in those days? From DHS's point of view, we ask a couple of fundamental questions.

First, what is the vulnerability? If this transaction occurred and the parties who are part of the transaction, who are making the acquisition intended to do us harm or some of them did, how much harm could they do with this acquisition? That is the first question we ask.

The second question we ask, not surprisingly, is do we have any reason to believe that the people who are engaged in this transaction, the company that is engaged in this transaction or the government that stands behind that company might wish to do any of those harmful acts.

So we look, first, at our vulnerability and then at the threat.

Once we have carried out that analysis, we have to decide, are we opposed to the transaction or are there risks here that could be minimized by changes in the practice of the company or by guarantees that the company wouldn't change its practice?

We often will ask companies for assurances that they are going to act in certain ways. These are called mitigation agreements, in which we mitigate the risk to national security.

We have been among the most active in seeking those agreements. All agreement with CFIUS in the form of mitigation agreements have increased. I think we entered into 13 during the first 3 years of our existence and last year we did 15 in 1 year alone.

Those mitigations and agreements have turned out to be quite useful and important to us. One of the things that we have also pioneered is going back and checking to make sure that the companies are carrying out their agreements.

There is nothing that concentrates people's mind so much as knowing that they are going to be audited on their performance and we have been active in auditing companies to make sure that they actually carry out their agreements.

This is something GAO noticed 2 years ago when they did the report on us. We have since established a formal unit that does nothing but audits, the first in government.

We are very proud of that record, and I am glad to answer questions about when the remainder of the witnesses have made their presentations.

Ms. JACKSON LEE. Thank you for your insightful and instructive testimony.

I now recognize Assistant Secretary Stephan to summarize his statement for 5 minutes.

Colonel, thank you very much.

STATEMENT OF COLONEL ROBERT STEPHAN, ASSISTANT SECRETARY FOR POLICY, DEPARTMENT OF HOMELAND SECURITY

Colonel Stephan. Madam Chairwoman, Ranking Member Lungren, other distinguished members of this subcommittee, thank you very much for the opportunity to speak to you today on behalf of my office, the office of infrastructure protection, to discuss our role in the CFIUS process in support of Assistant Secretary Baker.

Within the office of infrastructure protection at DHS, we carefully monitor and analyze the risk posed to the nation's infrastructure. Part of this analysis includes an assessment of foreign ownership, control and influence over our most significant critical infrastructures on a transaction-by-transaction basis.

Responsibility for this analysis rests jointly with the department's homeland infrastructure threat and risk analysis center, which is a combination of the office of infrastructure protection, with further outreach to other federal departments and agencies and other key players inside the department, as well as the office of intelligence and analysis.

HITRAC, as it is commonly known, develops tailored infrastructure-related threat and risk analysis products and monitors the changes to the threats, the vulnerabilities and the consequences associated with the nation's infrastructure that could affect the national risk profile.

Significant changes in the national risk profile will, in turn, drive changes in our operational focus, security plans and programs.

The HITRAC organization helps set the priorities for our collective infrastructure protection efforts from an analytical perspective. HITRAC also provides focused analytical support directly to the office of policy as part of the department's overarching role in the CFIUS process.

Although the policy office has overall responsibility for the department's CFIUS-related review process and for making recommendations to the secretary on how to approach each case, the dedicated staff in HITRAC support departmental decision-making by preparing risk assessments of every single filing for transactions and are provided directly to the office of policy.

These assessments, prepared by a specialized CFIUS support team of infrastructure and intelligence analysts within HITRAC, provide our policy decision-makers within the department an understanding of how these various potential acquisitions can impact, in a cascading manner, U.S. infrastructure.

HITRAC analysts conduct detailed reviews of all classified and unclassified information related to the foreign company of concern and subsidiaries involved in the transaction and look for indications that the foreign company and its senior personnel may have ties that could pose a threat to U.S. security, including ties with other foreign governments, foreign intelligence services, organized crime syndicates, or international terrorist organizations.

This research and analysis is supported by our law enforcement partners within DHS, such as ICE and CDP, as well as outside of the department, such as the FBI and others.

An assessment of the threat posed by foreign investors or owners, however, is only part of HITRAC's analytical capability.

HITRAC's CFIUS analysts work with subject matter experts in the infrastructure sector affected by a transaction to analyze the vulnerabilities associated within the U.S. infrastructure that the transaction may expose.

Obviously, situations in which the potential vulnerabilities can be exploited by identified threats raise significant concerns.

HITRAC then coordinates its analysis with relevant federal sector-specific agencies, such as the DHS Office of Cybersecurity and Telecommunications, the Transportation Security Administration, the U.S. Coast Guard, the Department of Energy, the Department of Defense, and various others.

The final risk assessment product informs the office of policy's recommendation to the secretary by highlighting areas of concern and increased risk and by proposing potential mitigation strategies the department may use to manage risk posed by the transaction.

Under the DHS chief intelligence officer, Charlie Allen's leadership, HITRAC's assessments also inform the director of national intelligence's reviews of each CFIUS case in collaboration with the other key elements of the intelligence community at large.

HITRAC provides analytical support and advice to the office of policy during negotiations on mitigation strategies that the U.S. government adopts to manage risk. It should be noted that HITRAC produces its assessments in a very compressed timeframe to allow policymakers maximum time to take appropriate action within the statutory 30-day initial timeframe and then the 45-day extended timeframe for presidential consideration.

In the year 2006, HITRAC reviewed 113 CFIUS cases, that is 113, writing coordinated assessments on each one. The CFIUS statutes prevent us from disclosing specific information about these cases in an open forum, but HITRAC's assessments have covered a wide range of infrastructures, to include chemical, energy, nuclear power sectors, to the information technology industry, to the defense industrial base.

Thus far in 2007, HITRAC analysts have reviewed approximately 30 cases, which is about a 20 percent increase over the same period of time from last year.

The office of infrastructure protection at HITRAC and its many partners recognize that thorough scrutiny of potential risk posed by foreign ownership of critical infrastructure is absolutely vital to our nation's security and economic strength.

We will continue to closely monitor CFIUS cases for the emergence of adverse trends and we will continue to work with our federal partners to ensure the performance of this mission meets with highest possible standards.

Madam Chairwoman, Ranking Member Lungren, I look forward to your questions. And, again, thank you for the opportunity to present my briefing to you today.

Ms. JACKSON LEE. Thank you very much for your testimony, Colonel. We will look forward to engaging you in questions that will allow you to give us your sense of the depth of the need of review of critical infrastructure. So we thank you for your testimony.

I now recognize Assistant Secretary Garcia to summarize his statement for 5 minutes.

Thank you very much.

STATEMENT OF HON. GREGORY GARCIA, ASSISTANT SECRETARY FOR CYBERSECURITY AND TELECOMMUNICATIONS, DEPARTMENT OF HOMELAND SECURITY

Mr. GARCIA. Madam Chairwoman, Ranking Member Lungren and distinguished members of the subcommittee, I appreciate the opportunity to briefly address you on our role, the Office of Cybersecurity and Communications, in the CFIUS process.

The Office of Cybersecurity and Communications, or CS&C, helps to ensure the security, integrity, reliability and availability of our information and communications networks.

Leveraging the subject matter expertise in CS&C, we evaluate transactions for potential vulnerabilities and the ensuing risk to the cyber and communications sectors, as well as other critical infrastructure sectors.

As appropriate, we provide risk mitigation advice and participate in post-action compliance reviews. This can include developing specific provisions in national security agreements between the U.S. government and the companies engaged in the transaction.

For example, from a cybersecurity and communications availability perspective, we would just need to closely review foreign ownership or management or service of telecommunications or IT services networks.

CS&C's role in the CFIUS process is a logical partnership as part of our work with cybersecurity and infrastructure protection. CS&C is engaged with the office of infrastructure protection, with Assistant Secretary Stephan, in incorporating cybersecurity and communications risk management processes throughout the national infrastructure protection plan, or the NIPP.

The NIPP requires each of the 17 critical infrastructures and key resource sectors identified in HSPD–7 to develop sector-specific plans and these plans address the physical, human and cyber elements critical to the proper functioning of that sector.

CS&C has a role in assisting sectors to address the cyber element by providing input to their sector-specific plans and developing cyber portions of risk management methodologies and supporting the protective programs that cut across all of those sectors.

CS&C also is responsible for the development and implementation of the information technology sector-specific plan and the communications sector-specific plan in coordination with the IT and communications industry partners and the government partners responsible.

That will conclude my comments. Thank you for the opportunity to appear before the subcommittee today, and I will be happy to answer any questions you have.

[The statement of Mr. Baker, Colonel Stephan and Mr. Garcia follows:]

PREPARED STATEMENT OF THE HONORABLE STEWART A. BAKER, ASSISTANT SECRETARY FOR POLICY, DEPARTMENT OF HOMELAND SECURITY

Madam Chairman, Ranking Member Lungren, Chairman Thompson, Ranking Member King and distinguished members of this Subcommittee, I am pleased to appear before you today to discuss the Committee on Foreign Investment in the United States (CFIUS)—of which the Department of Homeland Security is a member—and about the challenges posed by foreign ownership of critical infrastructure.

Background

I should emphasize at the outset that the CFIUS process is one of DHS's highest priorities. We have significantly increased staff and other resources and have a very robust review process that enables our Department to bring to CFIUS a diversity of viewpoints, expertise, and skills from across our constituent components. The government agencies from which we were formed give us a broad perspective, informed by a thorough understanding of infrastructure threats, vulnerabilities, and consequences.

Since the Department began functioning in March 2003, we have participated in the review of hundreds of foreign acquisitions, many of which have involved the nation's most critical infrastructure, technology, and other assets vital to our national security. In 2006, CFIUS reviewed over 100 transactions. DHS plays a particularly important role in CFIUS reviews of transactions involving critical infrastructure, and when DHS requests mitigation agreements in those cases—a topic to which I'll return in a few minutes—DHS has a leading role in monitoring compliance with those agreements to which they are a party.

DHS interprets its security mandate broadly. DHS's implementation of this mandate sometimes gives rise to debate within CFIUS, but it is a healthy debate that ultimately enhances both national security and an open investment climate—twin objectives DHS does not believe can be properly divorced from each other and which DHS always seeks to promote.

Jurisdiction

I want to highlight, however, that CFIUS is not a silver bullet capable of securing all critical infrastructure. In particular, Congress explicitly—and appropriately—limited CFIUS's legal authority to investigations of mergers, acquisitions or takeovers by or with foreign persons that could result in foreign control of persons engaged in interstate commerce in the United States. All CFIUS jurisdictional decisions are made based on a thorough evaluation of the specific facts presented by a given transaction.

Within CFIUS's statutory mandate,—that is, mergers or acquisitions that result in foreign control of U.S. businesses—our review is a searching one.

Our Review Process

DHS generally analyzes the incremental risk presented by an acquisition in three parts: (1) vulnerability; (2) threat; and (3) consequences.

The vulnerability analysis focuses on the assets being acquired. We ask, "what vulnerabilities are exposed by the transaction that may be exploited by someone with bad intent and significant capabilities" (this includes the company acquiring the U.S. operations as well as others who may take advantage of the new management). If a chemical plant is being acquired, for example, we want to know whether the chemicals produced are dangerous and, if so, whether there are significant vulnerabilities and if adequate security plans are in place to protect the physical facility and any sensitive data, systems, and networks.

The threat analysis then asks whether the acquirer has significant capabilities for exploiting the target and has intent to do so. Here we're looking for derogatory information about the buyer. The DNI coordinates preparation of a National Security Threat Assessment for each transaction by the intelligence community (including elements within DHS), which generally serves as the principal source of our threat analysis.

Finally, we ask what the consequences could be if the acquirer successfully exploited the target. To go back to the chemical plant example, we would want to know what would happen if someone exploited critical assets within the plant to cause an explosion or chemical release—how would that affect the surrounding communities? And we may need to know whether theft or exploitation of data, systems, and networks also could present a problem (e.g., within the chemical plant example: could the business systems be exploited to reveal HAZMAT routing information, or could the control systems be compromised to cause a dangerous chemical release?)

We then weigh these three factors—vulnerability, threat, and consequences—to come up with an assessment of the incremental risk presented by the transaction.

Background on Mitigation Agreements

In most transactions that CFIUS reviews, the increase in risk as a result of the foreign acquisition is either non-existent or sufficiently low that CFIUS needs to take no formal action. In other instances, we may see an increase in risk, but we may believe that existing authorities other than Exon-Florio and the International Emergency Economic Powers Act are sufficient to address the risk.

Occasionally, however, we come to the conclusion that the transaction may impair national security, that the incremental risk posed by the transaction cannot be adequately addressed by existing law, and that the risk can and should be mitigated

through a CFIUS agreement, as a condition to concluding the review or investigation without further action by the President.

A CFIUS mitigation agreement is an agreement between (i) companies undergoing a CFIUS review and (ii) and one or more of the CFIUS agencies. The purpose of such an agreement is to reduce the perceived national security risks associated with a foreign acquisition, merger, or takeover of a U.S. company subject to review by CFIUS. When the parties come to terms, a mitigation agreement generally will pave the way for the CFIUS agency or agencies involved to recommend that CFIUS allow the transaction to proceed.

Consistent with Exon-Florio and the important U.S. policy interest in maintaining an open investment climate, a CFIUS agency entering into a mitigation agreement seeks to mitigate national security risks using the means least onerous to accomplishing that end. Where CFIUS determines there is a risk to be mitigated, it takes a variety of approaches to mitigation agreements dictated by the particular circumstances of an individual transaction. They range from commitment letters on a specific issue of concern to formal mitigation agreements with detailed commitments including cooperation in the development and execution of security plans. As you would expect, agreements deemed necessary in transactions involving significant risks to critical infrastructure often are the most substantial. These agreements often include some combination of the following:

- Security plan and designated security officer
- Background checks for key personnel
- Limitations on foreign personnel's involvement in certain sensitive tasks
- Certification of export control compliance
- Customer lists
- Notifications of certain security incidents, such as cyber attacks
- Compliance with various appropriate international, industry, and/or Federal standards, guidelines, and recommended practices
- Right to site visits and access to books and records
- Audits
- Notification of changes to key management positions
- Liquidated damages for breach

Often the elements of these agreements—e.g., the requirements to have a security plan, security officer, conduct background checks, and comply with appropriate standards and recommended practices—reinforce measures already taken by the companies involved.

In rare cases, CFIUS agencies have asked the companies involved to agree to an "evergreen CFIUS" provision—i.e., the right to re-open a CFIUS case if the companies materially breach the mitigation agreement. The decision to re-open would be made by CFIUS consensus at the highest levels of each agency. DHS believes that this extraordinary remedy is appropriate in rare circumstances where the transaction presents significant national security risks, existing remedies will not be adequate to protect the national security, and we anticipate that standard commercial incentives will not be sufficient to compel compliance with the agreement.

Increase in Mitigation Agreements and Compliance Monitoring Work

Given the range of its responsibilities, DHS is often among the agencies which identifies the need to consider a mitigation agreement. Reflecting the increase in filings and other factors there has been a notable increase in the number of mitigation agreements.

Let me give you a few demonstrative statistics. From 2003–2005, the first three years of DHS's existence, we were a party to 13 mitigation agreements. In 2006 alone, DHS was a party to 15 mitigation agreements.

Of course, we recognize that when we enter into these agreements, we assume an obligation to monitor compliance. Our compliance monitoring is not new—GAO credited DHS's efforts in this regard two years ago. For some time DHS has:

- monitored to ensure that companies provide all reports and other deliverables required by mitigation agreements;
- reviewed all reports and other deliverables to ensure that they are accurate, complete, and otherwise satisfy the requirements of the agreements;
- occasionally conducted on-site visits and audits; and
- met with companies to discuss issues of compliance and non-compliance.

What is new, though, is that we?ve significantly increased the resources devoted to monitoring compliance. For example, whereas site visits previously were sporadic, DHS now has a program in place to conduct regular site visits.

We believe that DHS's CFIUS program represents a success story about the protection of critical infrastructure and other assets, and I would be happy to answer any questions you might have about the program

PREPARED STATEMENT OF COL. ROBERT B. STEPHAN

Madam Chairman, Ranking Member Lungren, Chairman Thompson, Ranking Member King and distinguished members of the Subcommittee, I appreciate the opportunity to briefly address you on our role in the Committee of Foreign Investment in the United States (CFIUS). Within the Office of Infrastructure Protection, we carefully monitor and analyze the risks posed to the Nation's critical infrastructure and key resources (CI/KR). Part of that analysis includes an assessment of foreign ownership, control and influence over CI/KR. Responsibility for that analysis rests with the Department's Homeland Infrastructure Threat and Risk Analysis Center (HITRAC).

HITRAC, a joint infrastructure-intelligence fusion center between the Office of Infrastructure Protection (OIP) and the Office of Intelligence and Analysis (I&A), provides tailored CI/KR threat and risk products to the private sector and our Federal, State, and local security partners. It monitors changes to the threats, vulnerabilities, and consequences associated with the Nation's infrastructure that could affect the national risk profile. Significant changes in the CI/KR risk profile will naturally drive changes in our focus, plans, and programs. HITRAC helps set the priorities for our collective critical infrastructure protection efforts.

HITRAC also provides focused analytical support directly to the Office of Policy as part of the Department's role on CFIUS. As you know, CFIUS is the interagency committee established in 1975 to review the national security impact of acquisitions, mergers, and takeovers of U.S. assets by foreign persons. DHS was added as a full member of the committee in February 2003 and joined eleven other members who deliberate each case in accordance with the Exon-Florio statute and applicable Treasury regulations.

Although the DHS Office of Policy has overall responsibility for the Department's CFIUS-related reviews and for making recommendations to the Secretary on how to approach each case, dedicated staff in HITRAC support Departmental decision making by preparing risk assessments of every filing that are provided directly to the Office of Policy. These assessments, prepared by a special CFIUS Support Team of OIP and I&A analysts within HITRAC, provide policy makers within the Department with an understanding of how these acquisitions can impact U.S. infrastructure.

HITRAC analysts conduct detailed reviews of all classified and unclassified information related to the foreign company and subsidiaries involved in the transaction, and look for any indication that the foreign company or senior personnel might, as the statute says, "take action that threatens to impair the national security."

This research is supported by our law enforcement partners such as Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP), which can provide evidence of potentially illegal trade practices and reach back to the broader law enforcement community.

An assessment of the threat posed by the transfer of control to foreign persons is, however, only part of HITRAC's analysis. HITRAC's CFIUS analysts work with subject matter experts in the infrastructure sector affected by a transaction to analyze the vulnerabilities in U.S. infrastructure that the transaction may expose. Obviously, situations in which the potential vulnerabilities can be exploited by identified threats raise the most serious concern. HITRAC coordinates its analysis with relevant Sector Specific Agencies, such as the DHS Office of Cyber Security and Telecommunications, the Transportation Security Administration, the U.S. Coast Guard, and the Department of Energy.

The final risk assessment informs the Office of Policy's recommendation to the Secretary by highlighting areas of increased risk and proposing potential mitigation strategies the Department can use to manage any risk posed by the transaction. Under DHS Chief Intelligence Officer Charlie Allen's leadership, HITRAC's assessments also inform the Director of National Intelligence's reviews of each CFIUS case, in collaboration with the rest of the Intelligence Community.

HITRAC continues to provide analytical support and advice to the Office of Policy during negotiations on mitigation agreements that the U.S. Government uses, in some cases, to manage risk. It should be noted that HITRAC produces its assessments in a very compressed timeframe to allow policymakers maximum time to take appropriate actions within the statutory 30-day timeframe mandated for initial CFIUS reviews.

HITRAC also performs similar analytical reviews of FCC license transfers to foreign entities through an interagency group made up of the Departments of Justice, Homeland Security and Defense.

In 2006, HITRAC analysts reviewed 113 CFIUS cases, writing coordinated assessments on each one. The Exon-Florio statute prevents us from disclosing information

about specific cases, but HITRAC's CFIUS assessments have covered a range of infrastructures, from the chemical, energy and nuclear power sectors, to the information technology industry, to the defense industrial base.

The Office of Infrastructure Protection and HITRAC recognize that thorough scrutiny of the potential risks posed by foreign ownership of critical infrastructure is vital to protecting the Nation's security and economic strength. We will continue to closely monitor CFIUS cases for the emergence of adverse trends, and we will continue to work with our Federal partners to ensure that performance of this mission meets with the highest standards.

Thank you for the opportunity to appear before this Subcommittee today and I would be happy to answer any questions you may have at this time.

PREPARED STATEMENT OF THE HONORABLE GREGORY GARCIA, ASSISTANT SECRETARY FOR CYBERSECURITY AND TELECOMMUNICATIONS DEPARTMENT OF HOMELAND SECURITY

Madam Chairman, Ranking Member Lungren, Chairman Thompson, Ranking Member King and distinguished members of the Subcommittee, I appreciate the opportunity to briefly address you on our role in the Committee on Foreign Investment in the United States (CFIUS). The Office of Cyber Security and Telecommunications helps to ensure the security, integrity, reliability and availability of our information and communications networks.

One area of particular emphasis for us is emerging cyber security threats. The Department reviews transactions notified to CFIUS for cyber security and communications threats and vulnerabilities. Leveraging the subject matter expertise in our Office of Cyber Security and Communications (CS&C), we evaluate transactions for potential vulnerabilities and ensuing risk to the cyber and communications sectors, as well as other critical infrastructures sectors. As appropriate given the nature of the transaction and subsequent risk, we assess vulnerabilities, participate in risk assessments, provide risk mitigation advice and participate in post-action compliance review. This can include developing specific provisions in risk mitigation agreements with the companies engaged in the transaction.

Our role in cyber security and infrastructure protection makes CS&C a logical partner in the CFIUS process. CS&C is engaged with the Office of Infrastructure Protection in supporting the cyber security and communications components of the National Infrastructure Protection Plan, which requires each of the 17 critical infrastructure and key resources sectors identified in HSPD–7 to develop Sector Specific Plans that address the physical, human, and cyber elements critical to the proper functioning of the sector. DHS/CS&C has a role in developing cyber portions of risk management methodologies and in supporting protective programs that cut across all sectors (e.g., US–CERT, the Control Systems Security Program). DHS/CS&C also is responsible for the development and implementation of the Information Technology and Telecommunications Sector Specific Plans in coordination private and public sector security partners.

Thank you for the opportunity to appear before this Subcommittee today and I would be happy to answer any questions you may have at this time.

Ms. JACKSON LEE. Mr. Garcia, thank you. We look forward to having an opportunity to question you this morning, and we appreciate your testimony.

I now recognize Ms. Calvaresi-Barr to summarize her statement for 5 minutes.

Thank you.

STATEMENT OF ANN CALVARESI-BARR, DIRECTOR OF ACQUISITION AND SOURCING MANAGEMENT, GOVERNMENT ACCOUNTABILITY OFFICE

Ms. CALVARESI-BARR. Thank you. Thank you, Madam Chairwoman and members of the subcommittee. I am pleased to be here today to discuss GAO's work on the Committee on Foreign Investment in the United States.

We have conducted many reviews of CFIUS since 1990 and have made recommendations directed towards improving the CFIUS

process. My statement today will address concerns from our 2005 report, recognizing that some actions are currently under way.

We are encouraged to hear of these efforts and appreciate the opportunity to recap our findings at this critical juncture in CFIUS's reform of the process.

Of concern to us were the fundamentally differing views among CFIUS members as to what constitutes a threat to national security, what criteria should be used to go to an investigation, and the sufficiency of time for reviews.

Regarding what constitutes a threat to national security, CFIUS members appeared to either view threats as limited to concerns about export controls, classified contracts, or specific derogatory intelligence against or about certain companies, or they viewed them more broadly in terms of vulnerabilities that can result from foreign control of critical infrastructure or critical inputs to defense systems.

For example, in one proposed acquisition, DOD raised concerns about the security of supply of its specialized integrated circuits, circuits that the Defense Science Board identified as essential to a number of defense systems, such as UAVs.

However, some CFIUS members argued that this was an industrial policy concern and, therefore, outside the scope of the Exxon-Florio statute.

As a result, a key enforcement provision that would allow the president to reopen a CFIUS review in the event of noncompliance was removed, which weakened the ensuing agreement.

CFIUS members also disagreed on the criteria that should be used to determine whether an investigation is warranted. Treasury and some other members used essentially the same criteria used by the president to suspend or prohibit an acquisition. That is, evidence that a credible threat exists and no other laws are adequate to deal with it.

However, officials from Defense, Justice and Homeland Security argued that applying these criteria is misguided, because isn't it the purpose of an investigation to, in fact, determine that a credible threat exists?

Disagreement among agency members on appropriate criteria for investigation can significantly impact the entire process. One notable case involved the acquisition of satellite technology.

Some members believed that an investigation was not warranted because the technology was unclassified and the country was an ally. Others, however, argued that the technology was defense critical and were concerned about third-party transfers.

While the case went to investigation, it was withdrawn and ultimately resulted in weak mitigation measures.

CFIUS members also disagreed about the sufficiency of time allowed for reviews. While most reviews are completed in the legislative timeframe, some agencies have faced significant time pressures to conduct reviews of certain cases.

In one case, Homeland Security was unable to provide any input within the legislative timeframe.

In addition to the differing views among members, our work revealed that CFIUS typically allowed companies to withdraw their notices in order to resolve concerns and avoid investigation. How-

ever, this can be particularly risky when the transaction has been completed and where national security issues have been raised. We found a number of such cases.

Avoiding investigations contributes to the opaque nature of the process, a concern repeatedly raised by Congress. Without an investigation, there is no presidential decision and no required reporting to Congress.

Given our findings, we made several recommendations. First, amend the Exxon-Florio statute to more clearly emphasize the factors that should be considered. Second, eliminate the distinction between review and investigation and make the combined period available for review.

Third, require an annual report on the nature of concerns for all transactions in the preceding year. Last, when using withdrawals, place interim protections and timeframes for re-filing.

Implementing Exxon-Florio in the context of open investment is a fine line to walk and presents significant challenges. Regardless of the sector in which a foreign acquisition occurs, the process needs to be effective.

While we remain optimistic that recent actions taken by CFIUS will help improve the process, we have not examined how these changes are working and strongly encourage any legislative effort that strengthens and sustains what is a key safety net in our national security framework.

This concludes my summary statement. My full statement has been submitted for the record. I would be happy to answer questions you or other subcommittee members may have.

Thank you.

[The statement of Ms. Calvaresi-Barr follows:]

PREPARED STATEMENT OF ANN M. CALVARESI-BARR

Madam Chairwoman and Members of the Subcommittee:

I am pleased to be here today to take part in this hearing on issues related to foreign ownership of U.S. assets and potential effects on national security. As you know, U.S. export control laws, national disclosure policy, the National Industrial Security Program, and other processes and programs have been established to protect defense technologies and other critical assets from falling into the wrong hands, and for other reasons. Similarly, the Exon-Florio amendment to the Defense Production Act of 1950,[1] enacted in 1988, authorized the President to suspend or prohibit foreign acquisitions, mergers, or takeovers[2] of U.S. companies that pose a threat to national security. Exon-Florio is meant to serve as a safety net when laws other than the International Emergency Economic Powers Act[3] may be ineffective in protecting national security.

Exon-Florio is administered by the Committee on Foreign Investment in the United States, currently made up of 12 members: the Department of the Treasury, which serves as Chair; the Departments of Commerce, Defense, Homeland Security, Justice, and State; and six offices in the Executive Office of the President. On the surface, the Exon-Florio review process is fairly straightforward. According to regulations, after a company voluntarily files a notice of a pending or completed acquisition by a foreign concern, the Committee conducts a 30-day review to determine whether there are any national security concerns. If the Committee is unable to

[1] 50 U.S.c. app. § 2170.

[2] In the remainder of this statement, acquisitions, mergers, and takeovers are referred to as acquisitions.

[3] The International Emergency Economic Powers Act gives the President broad powers to deal with any "unusual and extraordinary threat" to the national security, foreign policy, or economy of the United States (50 U.S.C. §§ 1701—1706). To exercise this authority, however, the President must declare a national emergency to deal with any such threat. Under this legislation, the President has the authority to investigate, regulate, and, if necessary, block any foreign interest's acquisition of U.S. companies (50 U.S.C. § 1702(a)(1)(B)).

complete its review within 30 days, the Committee may either allow the companies to withdraw the notification and refile or initiate a 45-day investigation. If a case undergoes an investigation, the Committee submits a report to the President, including a recommendation for action. Cases that result in a presidential decision are reported to the Congress.

As requested, my comments today will summarize our reports on weaknesses in the Exon-Florio process that GAO has identified over the past decade. Before I begin, however, it is important to provide some context to Exon-Florio. Specifically, implementing Exon-Florio can pose a significant challenge for the federal government because of the potential for conflict with U.S. open investment policy—a policy that, in recognizing the economic benefits associated with foreign investments, calls for foreign investors to be treated no differently than domestic investors. This challenge has increased significantly since September 2001, when threats facing the nation were fundamentally redefined to include threats against the homeland, including those to our critical infrastructure. At the same time, the economy has become increasingly globalized, as countries open their markets and communicate regularly through the Internet. Government programs established decades ago are often ill-equipped to grapple with these emerging complexities. GAO, therefore, designated the effective identification and protection of critical technologies as a government-wide high-risk area, which warrants a strategic reexamination to identify needed changes.[4] In terms of Exon-Florio, legislation has been introduced to reform the Exon-Florio process.

Our understanding of the Committee's process is based on our 2005 work but built on our review of the process and our discussions with agency officials for our 2002 report. For our 2005 review, and to expand our understanding of the Committee's process for reviewing foreign acquisitions of U.S. companies, we met with officials from the Departments of Commerce, Defense, Homeland Security, Justice, and the Treasury—the agencies that are most active in the review of acquisitions—and discussed their involvement in the process. Further, we conducted case studies of nine acquisitions that were filed with the Committee between June 28, 1995, and December 31, 2004. We conducted our review from April 2004 through July 2005 in accordance with generally accepted government auditing standards.

To summarize our work in this area, we have found that several aspects of the Committee's process for implementing Exon-Florio may have weakened the law's effectiveness. First, we found a lack of agreement among Committee members about the scope of Exon-Florio—specifically, what defines a threat to national security. Neither the statute nor the implementing regulation defines "national security." However, the statute provides factors that may be considered in determining threats to national security. Despite these factors, some Committee members argued to apply a more traditional definition?one limited to concerns about export-controlled technologies or items, classified contracts, and the existence of specific derogatory intelligence on a foreign company. Other Committee members have argued that a broader view is warranted, and in analyzing the effects of an acquisition, considered the potential vulnerabilities that an acquisition can create with regard to U.S. critical infrastructure, defense supply, and defense technology superiority. These disagreements may have limited the Committee's analyses of proposed or completed acquisitions.

Second, Committee members also had differing opinions on the criteria that should be used to determine whether an investigation was warranted. The criteria used by Treasury as the Committee Chair and others were essentially the same criteria established in the current law for the President to suspend or prohibit a transaction, or order divestiture—that is, there is credible evidence that the foreign controlling interest may take action that threatens national security and that no laws other than Exon-Florio and the International Emergency Economic Powers Act are adequate to protect national security. Some Committee members have argued that applying these criteria is inappropriate because the purpose of an investigation is to determine whether or not credible evidence of a threat exists.

Third, while most acquisitions are not problematic and the Committee's review can be completed within the 30-day period allowed by Exon-Florio, some more complex acquisitions required more analysis or consideration than the 30-day review period could accommodate. However, the Committee has been reluctant to use the additional 45 days allowed by the legislation because it would require initiating an investigation. The Committee's concern was that the negative perceptions surrounding an investigation could discourage foreign investment in the United States, thereby conflicting with U.S. open investment policy. To avoid investigations, the Committee has in the past encouraged companies to withdraw their notifications of proposed

[4] *High Risk Series: An Update,* GAO–07–310 (Washington D.C.: Jan. 2007).

or completed acquisitions and refile them at a later date. Between 1997 and 2004, companies involved in 18 acquisitions were allowed to withdraw their notification and refile at a later time. The new filing is considered a new case and restarts the 30-day clock. While withdrawing and refiling provides additional time for Committee members to review a foreign acquisition while minimizing the risk of chilling foreign investment, it may also heighten the risk to national security in transactions where there are concerns and the acquisition has been completed or is likely to be completed during the withdrawal period. This was the situation in 4 of the 18 acquisitions cited above. One company did not refile for 9 months, another did not refile for 1 year, and 2 had yet to refile at the time of our review.[5]

Finally, because very few cases required a presidential decision—the criterion for reporting to the Congress on specific cases—the Congress had little insight into the Committee's process. Further, a 1992 amendment to the legislation requires a report to the Congress every 4 years on certain trends in foreign acquisitions. However, at the time of our work only one report had been submitted, in 1994. I understand that another report, in response to that requirement, has been issued.

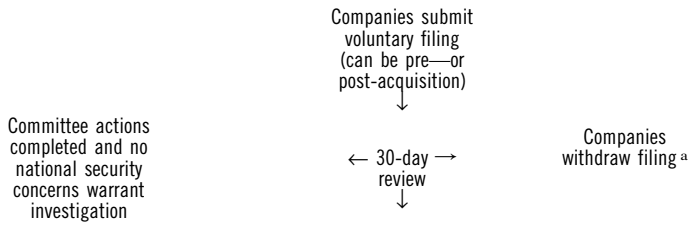
Since our 2005 report, the Committee has taken some actions to reform the process, such as increasing communication to interested congressional committees. However, we have not examined how these changes are working. It should be noted that because the law provides for confidentiality of information filed under Exon-Florio, our ability to discuss details of cases we examined is limited.

Background

Enacted in 1988, the Exon-Florio amendment to the Defense Production Act authorized the President to investigate the effects of foreign acquisitions of U.S. companies on national security and to suspend or prohibit acquisitions that might threaten national security. The President delegated investigative authority to the Committee on Foreign Investment in the United States, an interagency group responsible for monitoring and coordinating U.S. policy on foreign investment in the United States.[6] Since the Committee's establishment in 1975, membership has doubled, with the Department of Homeland Security being the most recently added member. In addition to the Committee's 12 standing members, other agencies may be called on when their particular expertise is needed.

In 1991, the Treasury Department, as Chair of the Committee, issued regulations to implement Exon-Florio. The law and regulations establish a four-step process for reviewing foreign acquisitions of U.S. companies: (1) voluntary notice by the companies;[7] (2) a 30-day review to identify whether there are any national security concerns; (3) a 45-day investigation period to determine whether those concerns require a recommendation to the President for possible action; and (4) a presidential decision to permit, suspend, or prohibit the acquisition (see fig. 1).

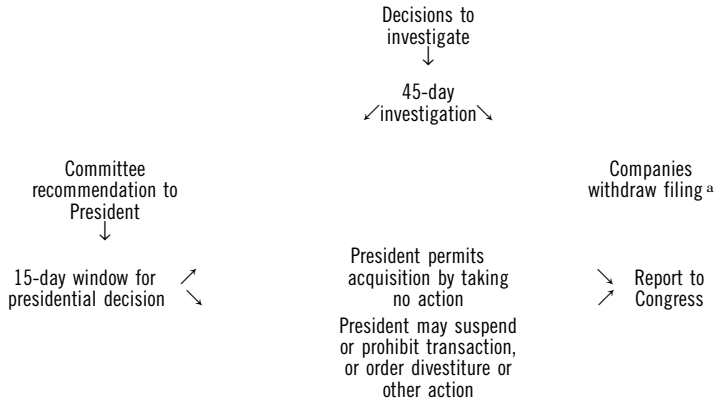
Figure 1: Process Used by the Committee on Foreign Investment in the United States to Implement the Exon-Florio Amendment



[5] Given the immediacy of this hearing, we were unable to gather and verify data on the disposition of these cases. However, even if the companies refiled subsequent to our 2005 reporting, the refilings were not timely.

[6] Executive Order 11858 (May 7, 1975), as amended by Executive Order 12188 (Jan. 2, 1980), Executive Order 12661 (Dec. 27, 1988), Executive Order 12860 (Sept. 3, 1993), and Executive Order 13286 (Feb. 28, 2003).

[7] Notification is not mandatory. However, any member agency is authorized to submit a notification of an acquisition if the companies have not done so. As of our 2005 report, no agency has submitted a notification of an acquisition. Instead, member agencies have informed Treasury of acquisitions that may be subject to Exon-Florio, and Treasury has contacted the company to encourage them to officially notify the Committee of the acquisition to begin a review.



Source GAO analysis based on 50 U.S.c. app. § 2170 and 31 C.F.R. Part 800 and case file reviews.

[a]**At any point prior to a presidential decision, companies can request to withdraw a notification.**

In most cases, the Committee completes its review within the initial 30 days because there are no national security concerns or concerns have been addressed, or the companies and the government agree on measures to mitigate identified security concerns. In cases where the Committee is unable to complete its review within 30 days, it may initiate a 45-day investigation or allow companies to withdraw their notifications. The Committee generally grants requests to withdraw. When the Committee concludes a 45-day investigation, it is required to submit a report with recommendations to the President. If Committee members cannot agree on a recommendation, the regulations require that the report to the President include the differing views of all Committee members.[8] The President has 15 days after the investigation is completed to decide whether to prohibit or suspend the proposed acquisition, order divestiture of a completed acquisition, or take no action.[9] Table 1 provides a breakdown of notifications and committee actions taken from 1997 through 2004 (the latest date for which data were available at the time of our 2005 review).

Table 1: Notifications to the Committee on Foreign Investment in the United States and Actions Taken, 1997 through 2004

1997	62	60	0	0	0
1998	65	62	2	2	0
1999	79	76	0	0	0
2000	72	71	1	0	1
2001	55	51	1	1	0
2002	43	42	0	0	0
2003	41	39	2	1	1
2004	53	50	2	2	0
Total	470	451	8	6	2[c]

Source: Department of the Treasury.

[a] Acquisitions that were withdrawn and refiled are shown in the year for initial notification.
[b] Investigations are shown in the year of their notification.
[c] In both cases the President took no action, thereby allowing the transaction, and sent a report to Congress.

Over the past decade, GAO has conducted several reviews of the Committee?s process and actions and has found areas where improvements were needed. In 2000, we found that gaps in the notification process raised concerns about the

[8] 31 C.F.R. § 800.504(b).
[9] In 1990, the President ordered a Chinese aerospace company to divest its ownership of a U.S. aircraft parts manufacturer. To date, this is the only divestiture the President has ordered.

CommitteeSs ability to ensure transactions are notified.[10] Our 2002 review, prompted by a lack of congressional insight into the process, again found weaknesses in the process. Specifically, we reported that member agencies could improve the agreements they negotiated with companies under Exon-Florio to mitigate national security concerns. We also questioned the use of withdrawals to provide additional time for reviews.[11] While our most recent work indicated that member agencies had begun to take action to respond to some of our recommendations, concerns remained about the extent to which the Committee's implementation of Exon-Florio had provided the safety net envisioned by the law.[12]

Views Differed over What Constitutes a National Security Threat and When an Investigation Is Warranted

In 2005, we reported that a lack of agreement among Committee members on what defines a threat to national security and what criteria should be used to initiate an investigation may have limited the Committee's analyses of proposed and completed foreign acquisitions. From 1997 through 2004, the Committee received a total of 470 notices of proposed or completed acquisitions,[13] yet it initiated only 8 investigations.

While neither the statute nor the implementing regulation defines "national security," the statute provides a number of factors that may be considered in determining a threat to national security (see fig. 2).

Figure 2: Exon-Florio Factors That May Be Considered When Determining a Threat to National Security

- Domestic production needed for projected national defense requirements.
- The capability and capacity of domestic indurstries to meet national defense requirements, including the availability of human resources, products, technology, materials, and other supplies and services.
- the control of domestic industries and commercial activity by foreign citizens as it affects the capability and capacity of the United States to meet national security requirements.
- The potential effects of the proposed or pending transaction on sales of military goods, equipment, or technology to any country identified under applciable law as (a) supporting terrorism or (b) a country of concern for missile proliferation or the proliferation of chemical and biological weapons.
- The potential effects of the proposed or pending transaction on U.S. international technological leadership in areas affecting national security.

Source 50 U.S.C. app. § 2170(f).

- Some Committee member agencies argued for a more traditional and narrow definition of what constitutes a threat to national security—that is, (1) the U.S. company possesses export-controlled technologies or items; (2) the company has classified contracts and critical technologies; or (3) there is specific derogatory intelligence on the foreign company. Other members, including the Departments of Defense and Justice, argued that acquisitions should be analyzed in broader terms. According to officials from these departments, vulnerabilities could result from foreign control of critical infrastructure, such as control of or access to information traveling on networks. Vulnerabilities can also result from foreign control of critical inputs to defense systems, such as weapons system software development[14] or a decrease in the number of innovative small businesses researching and developing new defense-related technologies.

While these vulnerabilities may not pose an immediate threat to national security, they may create the potential for longer term harm to U.S. national security interests by reducing U.S. technological leadership in defense systems. For example, in reviewing a 2001 acquisition of a U.S. company, the Departments of Defense and Commerce raised several concerns about foreign ownership of sensitive but unclassified technology, including the possibility of this sensitive technology being transferred to countries of concern or losing U.S. government access to the technology. However, Treasury argued that these concerns were not national security concerns because they did not involve classified contracts, the foreign company's country of

[10] *Defense Trade: Identifying Foreign Acquisitions Affecting National Security Can Be Improved,* GAO/NSIAD–00–144 (Washington, D.C.: June 29, 2000).

[11] *Defense Trade: Mitigating National Security Concerns under Exon-Florio Could Be Improved,* GAO–02–736 (Washington, D.C.: Sept. 12, 2002).

[12] *Defense Trade: Enhancements to the Implementation of Exon-Florio Could Strengthen the Law's Effectiveness,* GAO–05–686 (Washington, D.C.: Sept. 28, 2005).

[13] Nineteen of these notices were refilings.

[14] 14Defense Acquisitions: Knowledge of Software Suppliers Needed to Manage Risks, GAO–04–678 (Washington D.C.: May 25, 2004).

origin was a U.S. ally, or there was no specific negative intelligence about the company?s actions in the United States.

In one proposed acquisition, disagreement over the definition of national security resulted in an enforcement provision being removed from a mitigation agreement between the foreign company and the Departments of Defense and Homeland Security. Defense had raised concerns about the security of its supply of specialized integrated circuits, which are used in a variety of defense technologies that the Defense Science Board had identified as essential to our national defense—technologies found in unmanned aerial vehicles, the Joint Tactical Radio System, and cryptography and other communications protection devices. However, Treasury and other Committee members argued that the security of supply issue was an industrial policy concern and, therefore, was outside the scope of Exon-Florio's authority. As a result of removing the provision, the President's authority to require divestiture under Exon-Florio was eliminated as a remedy in the event of non-compliance.[15]

Committee members also disagreed on the criteria that should be applied to determine whether a proposed or completed acquisition should be investigated. While Exon-Florio provides that the "President or the President's designee may make an investigation to determine the effects on national security" of acquisitions that could result in foreign control of a U.S. company, it does not provide specific guidance for the appropriate criteria for initiating an investigation of an acquisition.[16] At the time of our work, Treasury, as Committee Chair, applied essentially the same criteria established in the law for the President to suspend or prohibit a transaction, or order divestiture: (1) there is credible evidence that the foreign controlling interest may take action to threaten national security and (2) no laws other than Exon-Florio and the International Emergency Economic Powers Act are adequate and appropriate to protect national security.[17] However, the Defense, Justice, and Homeland Security Departments argued that applying these criteria at this point in the process is inappropriate because the purpose of an investigation is to determine whether or not credible evidence of a threat exists. Notes from a policy-level discussion of one particular case further corroborated these differing views.

Committee Allowed Withdrawal of Notifications to Avoid Investigations

Committee guidelines required member agencies to inform the Committee of national security concerns by the 23rd day of a 30-day review—further compressing the limited time allowed by legislation to determine whether a proposed or completed foreign acquisition posed a threat to national security. According to one Treasury official, the information is needed a week early to meet the legislated 30-day requirement. While most reviews are completed in the required 30 days, some Committee members have found that completing a review within such short time frames can be difficult—particularly in complex cases. One Defense official said that without advance notice of the acquisition, time frames are too short to complete analyses and provide input for the Defense Department's position. Another official said that to meet the 23-day deadline, analysts have only 3 to 10 days to analyze the acquisition. In one instance, Homeland Security was unable to provide input within the 23-day time frame.

If a review cannot be completed within 30 days and more time is needed to determine whether a problem exists or identify actions that would mitigate concerns, the Committee can initiate a 45-day investigation of the acquisition or allow companies to withdraw their notifications and refile at a later date.[18] According to Treasury officials, the Committee's interest is to ensure that the implementation of Exon-Florio does not undermine U.S. open investment policy. Concerned that public knowledge of investigations could devalue companies' stock, erode confidence of foreign investors, and ultimately chill foreign investment in the United States, the Committee has generally allowed and often encouraged companies to withdraw their notifications rather than initiate an investigation.

While an acquisition is pending, companies that have withdrawn their notification have an incentive to resolve any outstanding issues and refile as soon as possible.

---

[15] The regulations provide that the Committee may reopen its review or investigation and revise its recommendation to the President if it determines that the companies omitted or provided false or misleading material information to the Committee (31 C.F.R. § 800.601(e)).

[16] 1650 U.S.C. app. § 2170(a). Under the statute, investigations are mandatory in those cases in which the acquiring company is "controlled by or acting on behalf of a foreign government" and the acquisition could result in control of the U.S. company and could affect the national security of the United States (50 U.S.C. app. § 2170(b)).

[17] 50 U.S.C. app. § 2170(e).

[18] Exon-Florio's implementing regulations permit companies to request to withdraw notifications at any time up to a presidential decision. After the Committee approves a withdrawal, any subsequent refiling is considered a new, voluntary notice.

However, if an acquisition has been concluded, there is less incentive to resolve issues and refile, extending the time during which any concerns remain unresolved. Between 1997 and 2004, companies involved in 18 acquisitions withdrew their notification and refiled 19 times. In four cases, the companies had already concluded the acquisition before filing a notification. One did not refile until 9 months later and another did not refile for 1 year. Consequently, concerns raised by Defense and Commerce about potential export control issues in these two cases remained unresolved for as much as a year—further increasing the risk that a foreign acquisition of a U.S. company would pose a threat to national security.

For the other two cases, neither company had refiled at the time we completed our work. In one case, the company had previously withdrawn and refiled more than a year after completing the acquisition. The Committee allowed it to withdraw the notification to provide more time to answer the Committee's questions and provide assurances concerning export control matters. The company refiled, and was permitted to withdraw a second time because there were still unresolved issues. When we issued our report in 2005, 4 years had passed since the second withdrawal without a refiling. In the second case, the company—which filed with the Committee more than 6 months after completing its acquisition—was also allowed to withdraw its notification. At the time we issued our report, 2 years had passed without a refiling.

Lack of Reporting Contributed to the Opaqueness of the Committee's Process and Diminished Oversight

In response to concerns about the lack of transparency in the Committee's process, the Congress passed the Byrd Amendment to Exon-Florio in 1992, requiring a report to the Congress if the President made any decision regarding a proposed foreign acquisition. In 1992, another amendment also directed the President to report every 4 years on whether there was credible evidence of a coordinated strategy by one or more countries to acquire U.S. companies involved in research, development, or production of critical technologies for which the United States is a leading producer, and whether there were industrial espionage activities directed or assisted by foreign governments against private U.S. companies aimed at obtaining commercial secrets related to critical technologies.

While the Byrd Amendment expanded required reporting on Committee actions, few reports have been submitted to the Congress because withdrawing and refiling notices to restart the clock has limited the number of cases that result in a presidential decision. Between 1997 and 2004, only two cases—both involving telecommunications systems—resulted in a presidential decision and a subsequent report to the Congress. Infrequent reporting of Committee deliberations on specific cases provides little insight into the Committee?s process to identify concerns raised during investigations and determine the extent to which the Committee has reached consensus on a case. Further, despite the 1992 requirement for a report on foreign acquisition strategies every four years, at the time of our work there had been only one report—in 1994. However, another report, in response to this requirement, was recently delivered to the Congress.

In conclusion, the effectiveness of Exon-Florio as a safety net depends on how the broad scope of its authority is implemented in today's globalized world—where identifying threats to national security has become increasingly complex. While Exon-Florio provides the Committee on Foreign Investment in the United States the latitude to define what constitutes a threat to national security, the more traditional interpretation fails to fully consider factors currently embodied in the law. Further, the Committee guidance requiring reviews to be completed within 23 days to meet the 30-day legislative requirement, along with the reluctance to proceed to an investigation, limits agencies' ability to complete in-depth analyses. However, the alternative—allowing companies to withdraw and refile their notifications—increases the risk that the Committee, and the Congress, could lose visibility over foreign acquisitions of U.S. companies. The criterion for reporting specific cases to the Congress only after a presidential decision contributes to the opaque nature of the Committee's process.

Our 2005 report laid out several matters for congressional consideration to (1) help resolve the differing views as to the extent of coverage of Exon-Florio, (2) address the need for additional time, and (3) increase insight and oversight of the process. Further, we suggested that, when withdrawal is allowed for a transaction that has been completed, the Committee establish interim protections where specific concerns have been raised, specific time frames for refiling, and a process for tracking any actions being taken during a withdrawal period. We have been told that some of these steps are now being taken.

Madam Chairwoman, this concludes my prepared statement. I will be happy to answer any questions you or other Members of the Subcommittee may have.

Scope and Methodology

Our understanding of the Committee's process is based on our 2005 work but built on our review of the process and our discussions with agency officials for our 2002 report. For our 2005 review, and to expand our understanding of the Committee's process for reviewing foreign acquisitions of U.S. companies, we met with officials from the Departments of Commerce, Defense, Homeland Security, Justice, and the Treasury—the agencies that are most active in the review of acquisitions—and discussed their involvement in the process. Further, we conducted case studies of nine acquisitions that were filed with the Committee between June 28, 1995, and December 31, 2004. We selected acquisitions based on recommendations by Committee member agencies and the following criteria: (1) the Committee permitted the companies to withdraw the notification; (2) the Committee or member agencies concluded agreements to mitigate national security concerns; (3) the foreign company had been involved in a prior acquisition notified to the Committee; or (4) GAO had reviewed the acquisition for its 2002 report. We did not attempt to validate the conclusions reached by the Committee on any of the cases we reviewed. To determine whether the weaknesses in provisions to assist agencies in monitoring agreements that GAO had identified in its 2002 report had been addressed, we analyzed agreements concluded under the Committee?s authority between 2003 and 2005. We conducted our review from April 2004 through July 2005 in accordance with generally accepted government auditing standards.

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

Ms. JACKSON LEE. I thank all the witnesses, and I thank you for your testimony.

I will remind each member that he or she will have 5 minutes to question the panel.

Let me also acknowledge the presence of Congresswoman Eleanor Holmes Norton. We thank her for her presence here.

And, Mr. Bilirakis, we thank you.

Before I recognize myself for questioning, without objection, I would like to insert into the record the Congressional Research Service report on "Exxon-Florio Foreign Investment Provision Overview of H.R. 556," from February 27, 2007, and Ms. Calvaresi-Barr's GAO report No. 05686.

See committee file.

Ms. JACKSON LEE. I will now recognize myself for questions.

First, Mr. Baker, I am interested in ensuring, this committee, I would hope is interested, and the full committee, Chairman Thompson and the ranking member, Mr. King, in being vigorous in anything that we do.

I think when we look at incidences like Madrid and like the London bombing, we know that, as I said earlier, we are telegraphed in what might happen.

Tell me how vigorous the Department of Homeland Security is in this process and, tell me, what is the missing element?

You, obviously, are the point person, meaning your office, when the call comes in that we are now engaged in the process. We have a transaction. The participants are anxious and we need to move quickly.

What is the framework that is used? And you might also answer, what is missing?

Mr. BAKER. Madam Chairman, thank you very much. It is an excellent question.

First, I should say we encourage companies to tell us long before they file that they are contemplating a transaction, so that we can

begin our work well before the 30 days begins, because 30 days is not enough time for a complex transaction with serious concerns. So often we will get the call well before a filing date.

But as soon as we get the call, we will assign one of our CFIUS experts to the case. They will being doing research on it. We will gather open source information about the transaction.

We will also alert the intelligence community and let them know about the transaction. We will let Bob Stephan know about the transaction so that they can begin looking at it, as well.

Once we get back some basic information on the parties to the transaction, the nature of the field, we will begin doing our analysis from the point of view of what our existing authorities are, what existing authority do we have to regulate the company to make sure that it does maintain high security standards.

If we think that there may be some gaps in our authority under existing law to address all of the potential concerns, we will begin asking, "Well, do we need a mitigation agreement to address those concerns?"

After 21 days, we will get an intelligence report that tells us whether there are any particular concerns about the company, its management, its ownership, the governments that it has close relationships with, and that will allow us to focus very carefully on particular threats.

At that point, we will put forward a mitigation agreement, if we think it is necessary, and often we will negotiate these deep into the night and overnight, because we usually have fewer than 3 or 4 days to get agreement on those.

While we can extend that, typically, a week or less is how long we will spend negotiating any agreement.

Ms. JACKSON LEE. I appreciate that scenario. What is missing? These agreements, these MOUs, are they missing, not included? Tell us what is missing.

Mr. BAKER. We are very glad that the House and this committee are looking hard at mitigation agreements, because, in fact, the statute doesn't have anything to say about mitigation agreements, even though we rely on them very heavily.

The statute didn't contemplate them. They are something that we have added to the process.

The new bill that is being considered here in the House would add the recognition of those agreements and give them force and enforceability in ways that will be very helpful to us.

Ms. JACKSON LEE. Thank you.

Colonel Stephan, do you think, in the work that you do, that we are not as conversant with the idea that critical infrastructures are vast and that there is a need for extensive oversight to ensure that elements that may include foreign investment are important to engage and to be able to assess the danger that they might pose?

Colonel Stephan. Yes, ma'am. We are very intricately involved with the process led by the policy office under the leadership of my friend, Mr. Baker, here.

I have dedicated an increasing number of my staff and an increasing amount of my time and energy actually to coalescing a specialized team of experts, infrastructure analysis, to deal with this issue.

I consider to be a very significant issue, something that we have to study very carefully and we have to provide the leadership in terms of the analytical piece.

One person that is missing here that is a key part of all this is Assistant Secretary Charlie Allen, with the INTEL and the threat slice. We have jointly agreed to combine a certain amount of our staff capability to focus on this problem.

In addition to the organic capability that we have in the department between Charlie Allen and I, depending on the nature of the infrastructure sets or subsets involved in any potential transaction, we also, through our guys, provide further outreach to the Department of Energy, Department of Defense, Department of Transportation, Commerce, others, to bring more analytical focus to the problem.

My piece of this isn't really too full. I have to determine what the possible vulnerabilities are on a sector-by-sector basis and on a cross-sector basis in terms of any proposed transaction and, secondly, I have to determine what the rippling, cascading consequences might if we have a bad actor that is, in fact, engaged in a process to acquire a particular infrastructure or system of infrastructures of concern to us.

Again, more and more brainpower from within my shop, more and more cases, we see the caseload growing about 20 percent to 30 percent a year over the past couple of years. So lots more time and talents from my shop focused on this, ma'am.

Ms. JACKSON LEE. Quickly, Ms. Calvaresi-Barr, we can't afford missteps, I believe, in this process, and I think oversight is important. What would you consider the major misstep or need for improvement pursuant to your report?

Ms. CALVARESI-BARR. I think that, as I mentioned before, it appears that there are certain changes that are currently under way.

I think some of the biggest concerns that we had are the factors that are considered when you look at a threat to national security and I think with the introduction and the involvement of the Department of Homeland Security in the process now, they have brought a new view to that and I think some of those things that were considered previously by the committee as sort of outside of the scope of Exxon-Florio are now getting increased attention as a result.

And I would like to just second what Mr. Baker said in terms of DHS's involvement in the process. We definitely did see more rigor, even in our 2005 review, over monitoring compliance with the agreements and putting some teeth into those agreements. So we were pleased to see that.

In terms of what is missing, you can see that in 2005, we had a number of findings and we had a number of concerns around not only the factors looked at, but the sufficiency of time and the extent to which these cases made it to a full investigation.

Since we haven't done work since that time period, I am not quite sure how things have improved, but I think we have heard here today from some of the recent numbers that the number of filings are up and, certainly, the number of mitigation agreements also appear to have increased.

But, again, GAO has not looked at the implementation of some of those actions since our 2005 work.

Ms. JACKSON LEE. I thank the witness.

And I yield to the distinguished gentleman from California, Mr. Lungren.

Mr. LUNGREN. I thank you very much, Madam Chairwoman.

Secretary Baker, you mentioned that you folks are the junior ones, that is, most recently formed. You didn't exist with the CFIUS process first started.

One of the concerns some people expressed during the Dubai controversy was whether or not the DOD and Homeland Security were sufficiently—their concerns were sufficiently taken into account.

How does the process work in that the secretary of treasury is the top guy? And the legislation we have that would make the homeland security secretary the vice chair of that, something we think is good, but is that mere window dressing or would that actually make a difference in terms of the way the considerations are made and the final decision is made?

Mr. BAKER. Thank you, Ranking Member Lungren.

Treasury is the chair and I know there have been times in the past when treasury has been criticized as taking into account too much the concerns of investors and not enough the concerns of national security agencies.

We have no complaints of that sort. The Treasury Department has been an evenhanded and fair-minded broker as difficult issues have been thrashed out.

The House bill does propose, I think, to make the Department of Homeland Security a vice chair of the committee. To tell the truth, we have doubts about how valuable that would be in terms of putting us in a different position from the position we are in now.

We have a substantial amount of authority to pursue our own interests and where the entire government has to be involved. We have to persuade the rest of the agencies that we are right and I don't think any of that would change if we were the vice chair.

Mr. LUNGREN. Can you tell me how many DHS employees work on CFIUS issues?

Mr. BAKER. It would be hard to give you an exact number, because we rely heavily on other parts of the agency, but it is certainly in double figures. We have a number that work directly for me. HITRAC has dozens of people who, at one time or another, we would draw on for this.

Mr. LUNGREN. Do you need additional resources in order to do this job, since we are having an increase in the number of applications and considerations?

Mr. BAKER. We have increased our resources for this and I believe the 2008 budget request from the administration also reflects the request for additional resources.

So, yes, we would be delighted to get more resources.

Mr. LUNGREN. When CFIUS was first created under President Ford, at his direction, we were still in the Cold War. We basically were looking at other countries with an aspect towards their alignment in the Cold War.

We now have a situation in which international terrorism is a major concern, if not the major concern. Things can change quickly

in terms of governments, in terms of the political dynamic in a particular country.

Is there a review process such that after a review has taken place, with or without mitigation agreements, that 2 or 3 years down the line, we take into consideration the change in a government or the change in the influence of terrorist operatives with respect to particular economic interests that may be involved with an agreement that has been made?

Mr. BAKER. That is a very good question. If the transaction was passed without a mitigation agreement, the general view has been we should not let markets think that we will be constantly interfering in the transaction.

In fact, the principal reason people file in CFIUS is to get the good housekeeping seal of approval that means we won't go back and reopen the deal.

But if there has been a mitigation agreement, we do have authority to go back and see how it has been performed.

Mr. LUNGREN. How do you enforce that?

Mr. BAKER. Well, we have been writing in tougher and tougher provisions to these agreements and—

Mr. LUNGREN. So how do you enforce the tougher and tougher elements?

Mr. BAKER. Well, we can order people to obey. These days, typically, we will ask for fine authority up to 15 or 20 or 30 percent of the actual value of the transaction, which certainly concentrates people's minds.

In very rare cases—

Mr. LUNGREN. Has that ever occurred?

Mr. BAKER. Have we ever assessed a fine?

Mr. LUNGREN. Yes.

Mr. BAKER. No, we have not.

Mr. LUNGREN. Have we ever threatened to assess the fine?

Mr. BAKER. We have not had to threaten to assess the fine, but we have had circumstances in which someone we believed had not been fully compliant with past agreements, where that has been a factor in our decision to say, "You know, this next transaction you want to do, don't do it."

Mr. LUNGREN. Thank you very much, Madam Chairwoman.

Ms. JACKSON LEE. Thank you very much, Mr. Lungren.

I am now pleased to yield 5 minutes to the distinguished gentlelady from New York, Ms. Clarke.

Ms. CLARKE. Thank you, Madam Chair, Ranking Member Lungren.

Good morning to each of you, and thank you for your testimony here today.

As the world economy increasingly globalizes, it is important that the United States pay close attention as to how this could impact on our homeland security.

I come from New York City. I am a native New Yorker and it is indeed the most global city on the earth. Every day, as markets shift, as companies buy and sell goods and services, as new businesses open and old companies are sold, there is more international commerce in New York than anywhere else.

Therefore, the issue of foreign ownership's impact on homeland security is not just a question of protecting our homeland, but for me and my constituencies, also a question of protecting my hometown.

Though CFIUS was created to ensure that foreign investment or ownership of U.S. companies and infrastructure would not adversely affect America's security, the debacle that occurred last year over management of U.S. ports puts the work of CFIUS into question.

At that time, the nation learned that the approval process is highly secretive, that there is little input from the outside or no input from Congress.

We also learned that the process must happen so quickly that the committee often fails to perform full investigations.

If this is not changed, someday a detail will be missed and America's security will be put at risk.

Mr. Baker, I want to ask, we have heard from your testimony that disagreement over the definition of national security has led to enforcement problems. In the past, some members of CFIUS have felt that it is OK to allow a foreign company to have sensitive government technology and other secrets and have decided that CFIUS should not get involved in an industrial policy concern.

Other members of the group, such as DOD, have had strong reservations about this information getting out.

How does the department define national security in this context?

Mr. BAKER. Thank you, Representative Clarke. My hometown too. I went to PS–196.

I think that that is an excellent question and one that each agency, at the end of the day, answers for itself. So I can only speak for the Department of Homeland Security.

We take a very broad view of what national security entails. WE have to ask how could a creative enemy use this capability, this investment against us and what can we do to make sure that we have made the company and the assets as secure as possible after the transaction.

And we are not limited to a Cold War view of national security or a purely governmental view of national security. If we think the terrorists could misuse access to an asset by virtue of a transaction, then we will ask for action to make sure that that security hole is closed.

Ms. CLARKE. Has there been any discussion about whether, in fact, a standard, a bar should be set amongst the agencies that would interact with respect to these transactions?

Mr. BAKER. That has been discussed, but there are some difficulties with that from both the point of view of the people who have a narrower view of national security and from our point of view, as well.

Homeland security concerns a lot of things. The food supply of the country, obviously, implicates homeland security. But that doesn't mean that we want to regulate every time a farm is bought by somebody from outside the country and we wouldn't want to imply that we were. At the same time, we wouldn't want to exclude agriculture and farming from our definition of homeland security.

So we have had to play it, to some extent, by ear and be flexible about particular transactions. So I would not suggest that we set a standard, because we could end up constrained by it or creating something that arouse unnecessary fears in investors.

Ms. CLARKE. And let me just ask, are you at all concerned about foreign companies and governments having control over highly sensitive American technology?

Mr. BAKER. Yes. You have to look at the particular technology. We are an importer of technology, as well as a developer of technology these days and we want to be able to invest abroad in technology firms.

But there are some technologies where the U.S. has a lead and it is important to our security and we should continue to maintain that lead.

Ms. CLARKE. Thank you for your responses to these questions. And I did detect a little New York accent.

Thank you, Madam Chair.

Ms. JACKSON LEE. Thank you for your constructive questioning, Ms. Clarke, and thank you for your noting your relationship between the PSes around here, public schools.

Mr. LUNGREN. Could I ask a question, as a westerner? Is there a single New York accent? I am surprised.

Ms. CLARKE. I think Brooklyn kind of supersedes every other part of the city.

Ms. JACKSON LEE. We will make sure the clerk is getting that exchange. Thank you.

Mr. Bilirakis, I don't know if there is a Pennsylvania accent, but we are delighted to yield to the distinguished gentleman for 5 minutes.

Mr. BILIRAKIS. We have got a little Florida, a little Pennsylvania, a little Greek, whatever works. Thank you.

Ms. JACKSON LEE. And it is Mr. Bilirakis of Florida, as he has noted.

Mr. BILIRAKIS. Although my dad is from Pennsylvania.

Ms. JACKSON LEE. I know that.

Mr. BILIRAKIS. Secretary Baker, I have one question.

In your written testimony, you state that the Committee on Foreign Investment in the United States' authority is limited to investigations of mergers, acquisitions or takeovers by or with foreign persons that could result in foreign control, or persons engaged in interstate commerce in the United States.

You have touched on this. Should the committee's authority be expanded and if so, do you have any recommendations on expansions of that authority which could be beneficial to the review process?

Mr. BAKER. On the whole, expanding the authority would greatly expand our workload and the concerns among investors in whether their transactions are going to be covered, and I am not sure it would give us much more clout in investigating risks to national security.

We have the authority to say, "You are calling this a lease, but we think it is, in fact, an acquisition. You are calling it a loan. We think it is really an acquisition."

So we have a fair amount of authority where we think national security is involved and that there really is a transfer of control. And so we have not felt that we needed more authority to investigate a number of things that could turn out simply to be ordinary commercial transactions.

Mr. BILIRAKIS. Thank you.

Thank you, Madam Chair.

Mr. LUNGREN. Would the gentleman yield? If I could ask a question on your time of Mr. Garcia.

That is a concern that I and other members of this committee and subcommittee have expressed over time has been that both in the private and the public sector, we haven't taken sufficient notice of the importance of cybersecurity, that is, the cyber world embedded in so much of what we do.

Since that is a general observation, can you tell us whether you are satisfied that CFIUS, as presently constituted, appreciates the role of the cyber world in these questions of critical infrastructure and whether or not they have manifested the technology understanding and fix to make those kinds of issues sufficiently reviewed in this overall process?

Mr. GARCIA. Yes, sir. Thank you for that question, Congressman.

Yes, I am satisfied and I think it is important to note that the threats and vulnerabilities facing our communications and cyber infrastructures are constantly evolving. So we need to constantly evolve our understanding and awareness of those vulnerabilities.

And my office, working in partnership with Secretary Baker and Secretary Stephan, looks really at two things. First, the extent to which an acquisition will result in or exacerbate vulnerabilities in the communications or cyber infrastructures specifically, but also the extent to which those cyber and communications infrastructures can be used to create vulnerabilities or threats against physical infrastructures.

As you alluded, our cyber and communications infrastructure is a foundation, an operational foundation for virtually every one of the critical infrastructure sectors. We depend on those communications and cyber infrastructures in order for us to do our work in all of the others.

So to the extent that any acquisition may result in additional vulnerabilities to those physical infrastructures through control systems or other vulnerabilities, we have a direct role and have participated in the CFIUS process to identify what those vulnerabilities are.

Mr. LUNGREN. I thank you.

I thank the gentleman for yielding the time to me. Appreciate it.

Mr. BILIRAKIS. Thank you, Madam Chair.

Ms. JACKSON LEE. Thank you very much, Mr. Bilirakis.

I am now delighted to yield 5 minutes to the gentlelady from the District of Columbia, Ms. Eleanor Holmes Norton.

Ms. NORTON. Thank you, Madam Chair.

Ms. JACKSON LEE. Who is in a battle all of her own about the critical infrastructure of voting. We look forward to that moving forward.

Ms. NORTON. That is going to be over soon with a victory.

Madam Chair, this is an important hearing and I am very pleased you have called it and called our attention to it.

Just before I get to my CFIUS question, could you give me some context here?

The context I need has a lot to do with the Open Skies Treaty, which is still very controversial in another of my committees. It is still is going nowhere, in part, because of security concerns.

I think everybody has come to grips with the fact that this is both a global economy and a technological economy all happening at the same time. We are talking about investments, transactions that normally the government would have nothing to do with. They have to occur in real time.

Give me some context. Does the United States have ownership, a fair amount of ownership in the critical infrastructure of other countries and if so, what have they done to protect, quote, themselves, not from us, but form the same concerns we have?

Mr. BAKER. I don't have the exact figures, but, yes, I think that, first, probably 80 or 90 percent of the critical infrastructure of the United States is in private hands and similar numbers are probably true throughout the Western world, and a number of our companies are big investors abroad, whether it is IBM or General Electric.

They own large chunks of the infrastructure?

Ms. NORTON. They must own those in countries that have not only similar concerns, but, frankly, some of them certainly in Europe—

Mr. BAKER. That is right.

Ms. NORTON. —had more, if I can call it, experience with terrorism than we have.

Have you learned anything from them? Have they proceeded smoothly in this way, with or without something comparable to CFIUS?

Yes, Ms. Barr?

Ms. CALVARESI-BARR. Yes. You might be interested to know that we were pressed by Senate Banking to actually look at foreign direct investment in other countries, the extent to which other countries have national security reviews, are they similar to what the United States has? How do they differ, if they differ? Are we being too rigorous, things of that nature.

So just I response to that, I think, clearly, other countries do have national security reviews. From work that we did previously on this issue, it is rather dated now and that is why we have been asked to come back in and look.

Some of them kind of look like our process. Others are little bit more rigorous and some are a little bit lighter.

So we are going to go back in and we are going to take a look and do a current assessment of what those other national security?

Ms. NORTON. I would appreciate it. They have been more vulnerable and closer to the sources of concern and, in some ways, they have been ahead of us on security, witness, what somehow we took credit for, but clearly was entirely a British matter and that is the plane or the terrorist that almost got on the plane that came here.

They just caught him and it was extraordinary to see.

I really have questions about cybersecurity in light of the pace of technology. I mean, it is kind of pitiful when we see Congress try to regulate in a technological area, because it is very hard to do.

It is very hard to do, because whatever you are regulating right from under you can change and that is inevitable.

What concerns me is that given that changing pace, I would have to assume, in the cybersecurity area, that the United States of America is not always ahead of the game, ahead of the curve.

I have no reason to believe that other science, for example, in the technological area is not, in some cases, even more advanced.

Let me just give an example that has no relevance. I understand that Southern Europe laughed at our cell phones, because they consider them so backward.

Perhaps we are further ahead when it comes to other technology or the technology we are concerned about. But I have no reason to believe that we are ahead in terms of the scientific thinking of the Japanese, the Chinese or the Europeans.

So here we are looking at cybersecurity at a moment in time and I understand what you said about not essentially monitoring this every other moment. So with the changing nature of technology, with the unknown there, I am not sure why we should feel secure in the cybersecurity area, unless there is some way to keep track of whether people who are—if you will forgive me—ahead of us I a number of technological areas, why we shouldn't assume that all kinds of things could happen that no one even dreamed of, not investigated, even dreamed of.

That is what technology is about today.

If you would tell me why I should feel safe and secure in light of those changes, I would be happy to hear it.

Mr. GARCIA. Yes, Congresswoman, I would be delighted to take a stab at that.

First of all, my belief is that the United States is the most technological innovative country in the world.

Ms. NORTON. Well, you know what? That is the kind of hubris that could get us in trouble. Even if that is the case, there is no reason to believe, given the changes and given our allies and some who are not our allies, that that is, indeed, what we are up against.

It seems to me, as security officials, your job is to assume the opposite, to assume that some other country, perhaps not the most secure, for that matter, some other investor, could get ahead of us, at least temporarily.

Would you give us at least that in the security area?

Mr. GARCIA. Absolutely. And my next point was to be that while we are technologically innovative, so, too, in the world of cybersecurity, are our adversaries.

We are acutely aware that there are increasing levels of sophistication among the adversaries as it pertains to the ability to exploit vulnerabilities in our communications and cyber networks.

So we are constantly—it is, in fact, a technological chess game. For every innovation that we have to better secure our networks, the hackers and other adversaries find ways to exploit—

Ms. NORTON. See, how don't see you how you monitor that kind of stuff. Hackers, changes that are legitimate and that may be trade secrets, I think—

Mr. GARCIA. We are constantly monitoring networks for anomalous activity and analyzing what types of vulnerabilities are being exploited with what attacks, but I hasten to add that the issue of cyber and communications security is not just a technological one.

We can have the best technology in place, but if we don't have appropriate systems and appropriate training of the people using those systems, then we are not going to really be truly secure.

Cybersecurity is really about three things: It is about technology, it is about people, and it is about process. And in the CFIUS process, we are looking not only at the technological vulnerabilities, but some of the basic questions we ask are, in this particular acquisition, does the acquiring or the acquired company have good cybersecurity policies in place?

Do they have a person who is in charge of implementing and enforcing those cybersecurity policies? Are there sufficient controls on access to the systems and on access to the data? Is there good personnel security? Does the company or companies have good background checks on possible insiders who could do malicious attacks on the networks?

What about the physical or environmental security surrounding a particular facility? What about employee training? Is everyone using the network fully aware of what they should and should not do in managing their information and their computer systems?

Does the company have a good monitoring and incident response capability in the event something bad does happen? Do they have a disaster recovery business continuity process?

Ms. NORTON. So the major technological change that was not contemplated either in the CFIUS review or, for that matter, in the imagination, because that is where technology is going, and is there some way in which that would be either be detected or reported to you?

Mr. GARCIA. We are constantly monitoring changes in technology and working with the private sector to identify the kinds of vulnerabilities that can—

Ms. NORTON. So when somebody hacks into a system, would you know that?

Mr. GARCIA. Yes. In my organization is an operational strike team, called the USCERT, the computer emergency readiness team. This is a group of technical professionals who have a network of outreach, incident response, situational awareness capabilities with other federal agencies, with other private sector operational capabilities, federal, state, local, and international partners.

So we are constantly, in real time, monitoring all of the activity, as much as the activity as we can on networks and—

Ms. NORTON. I appreciate your answer. Could I just ask whether or not, Ms. Barr—since GAO has had an opportunity to look at this system? If she could just respond.

Ms. JACKSON LEE. Answer the gentlelady's question briefly.

Ms. CALVARESI-BARR. Yes. I would be happy to respond. I am not a cybersecurity expert.

We reviewed the CFIUS process. I will tell you that the cases that we looked at, now rather dated, though, 1995 running through 2004, we did find instances where there were concerns raised about purchases of Internet backbone companies.

This predated a lot of DHS's involvement, because they weren't involved in those cases at the time. But I can tell you that some of those foreign acquisitions did pose a threat, one that didn't always get addressed to the satisfaction of other members of the committee or mitigated.

But I will note that I think the addition of DHS to the CFIUS committee has brought a new vigorous look in that area.

Ms. NORTON. I want to thank you again, Madam Chair. And I do want to say that I think this area deserves very special oversight just because we are all talking about what we don't know anything about.

It is the unknown that concerns me and I appreciate what is being done to close those concerns. And I appreciate it, again.

Ms. JACKSON LEE. Well, the gentlelady from the District of Columbia probably has firsthand knowledge, as the gentlelady from New York, on what terrorism can do to a community and, certainly, I believe these questions are valuable and important.

I am going to ask a few more questions in a second round and I respect my members, but my preface to this is this is the beginning of a series of hearings because we believe in the cruciality of vigorous oversight.

Ms. Calvaresi-Barr, we may be posing to GAO a study after the fact, which is to assess CFIUS with DHS engagement and involvement.

The three secretaries—and, Mr. Garcia, I am going to pose a question to you, because I believe that there is such a nexus in the knowledge which most Americans probably would not know that 80 to 90 percent of critical infrastructure is in private hands.

They also might not understand that there is a question of whether or not investment should also be equated to acquisition. And I will be raising that question with Mr. Baker, because there are entities where there is an operational factor, where there is a 70-or 80-year lease and the lease is paid up front.

There are questions that we have not, I think, asked or answered.

I would also argue whether revenue and buying and selling is more important than the security of America. And before this time, as Ms. Clarke has indicated, we are cities of commerce. We compete to be cities of commerce. We compete to account, through local officials and others, we account for or seek bragging rights of how much foreign investors we can secure for our own community, to sometimes the disadvantage of our own citizens who live here that we are willing to, for example, sell tow ropes and lease them up front—when I say "sell them," in a leasing procedure.

And having experienced not a manmade disaster, but a natural disaster, right after Katrina, when Rita panicked the Gulf region and we saw thousands upon thousands, Colonel Stephan, of individuals trying to escape by way of cars.

If, by some chance, the foreign operator that road had another idea, another scheme, another method of traveling on that road or

we don't want to alter or participate in your evacuation process, and that is for a natural disaster, then are we yielding to the buck of selling off roads and bridges, which I believe, under the present scheme of things, don't get covered by CFIUS?

And I would imagine Mr. Garcia will say some aspects of what he does and I am going to pose this first question, Mr. Garcia, because you are crucial. I am thinking of companies that are sending data from one foreign site into the United States.

Again, that may be questionable whether CFIUS has some role in determining whether that transaction is breaching any security, but it is using a very important aspect of critical infrastructure.

So I would like to ask a question that, as you have stated, the emerging threats to our infrastructure arising from cyberspace pose an interesting problem to contend with.

Can you please comment on how you see the CFIUS process evolving, especially software manufacturing and how it could move to offshore locations, whereby malicious code could be installed and do you have any suggestions for how to address these concerns?

Mr. Garcia?

Mr. GARCIA. Yes, Madam Chairwoman, an excellent question.

The issue you refer to we call the globalization of information technology and the IT sector is extremely globalized in terms of services, management, supply chain.

Recently, an interagency committee prepared a review of the globalization of IT and the extent to which there are vulnerabilities in a global supply chain in which, as you suggest, malicious code can be inserted into software that is developed overseas.

And we are looking at that closely and talking to the software industry, understanding that what is paramount is exactly how does a software company go about managing the development of software in a secure way, regardless of where the software is developed.

Malicious code can be inserted anywhere by anyone along the development supply chain.

So what is of most importance is working with the industry to devise best practices for secure development of software and hardware systems that are being used in our critical infrastructure.

Ms. JACKSON LEE. I think there are many scenarios. Of course, we don't want to telegraph of provide incentives to terrorists, but even the question of foreign investment by the United States, United States companies, and they then have to communicate back to the home office or the home office has to communicate back to them in a foreign site, which then some malicious code may undermine, for example, oil transactions or natural resource needs, water needs.

Again, this, I believe, points out, from my perspective, that the security of America is far more important, though we must balance it with the making of a buck.

And my concern is or my question is, and let me have Colonel Stephan in it, but let me let you finish, I am really contemplating of a more vigorous role for DHS, Secretary Baker, in this process.

Secretary Garcia?

Mr. GARCIA. Yes, ma'am. We 100 percent agree. The most important priority for the Department of Homeland Security is the homeland security, regardless of who benefits from an investment.

We look very closely at both the communications and cyber infrastructures as subjects of acquisition, but also how those infrastructures can be used against other physical infrastructures.

One of my organizations—

Ms. JACKSON LEE. Do you believe we should be vigorously involved in this process?

Mr. GARCIA. Yes, ma'am. One of my organizations is the national communications system, which is responsible for ensuring the availability of our communications infrastructure in times of national emergency, that our government decision-makers actually have an ability to communicate in the event of a national emergency.

To the extent that any acquisition, foreign acquisition of telecommunications infrastructure would, by our analysis, threaten our ability to have that communication in the event of a national disaster of any sort, we would take the appropriate steps to ensure that controls are put in place or not to permit at all.

Ms. JACKSON LEE. Colonel Stephan, can you explain and give an example of how your office works with Secretary Garcia's office to address and mitigate physical and cyber-related threats to infrastructure, including any recent example that is not classified?

Colonel Stephan. Yes, ma'am. In the CFIUS process that is the subject of this hearing, again, my responsibility is coordinating the infrastructure analysis or analytical components—

Ms. JACKSON LEE. So you are the firefighter that jumps into the fire?

Colonel Stephan. I am an integrator and coordinator and sometimes I get burned in the process.

Ms. JACKSON LEE. I don't want you to have that happen to you. But when you get the call, you have to move forward to make the analysis.

Colonel Stephan. Yes, ma'am. We make the analysis and we call in, depending upon what the transaction involves, a cyber component, a component of the energy sector. I bring in the Department of Energy, the Department of Defense, the defense industrial base.

So I am a coordinator and integrator of a very complex ballet across the United States for every one of these risk analysis pieces.

We just completed a round of very important, I think, pioneer work in terms of the public-private sector partnership, in my world, infrastructure protection. We now have 17 sector-specific plans that reflect the 17 infrastructure sectors designated in HSPD–7.

My colleague here and his staff have the unenviable task of reviewing every single one of those plans to make sure that the cyber components specifically dealing with control, processes, mechanisms and protocols for physical infrastructures that have a tremendous cyber component to each and every one them, was thoroughly involved in the process of developing the cyber pieces of every chapter of those plans.

So I think that would be a very positive example of some very comprehensive legwork that my partner, Assistant Secretary Gar-

cia, and his team and some very valuable capability they added into the fight.

So for our chemical plan, our nuclear energy sector plan, our energy sector plan, very large, his guys' eyes on every one of those individual prizes to make sure that the cybersecurity component was embedded inside those physical infrastructure—

Ms. JACKSON LEE. Colonel Stephan, we will be seeking copies of those plans and, frankly, you have laid out the agenda for this committee. We will, in fact, be looking at all of those sectors and so you will be hearing from this committee to secure those plans, as well.

I know the time—let me try to quickly go to Ms. Calvaresi-Barr and then to Mr. Baker. And I will let you finish, Mr. Garcia, because you may want to answer on how you coordinate with Colonel Stephan.

But, Ms. Barr, I, frankly, believe that the DHS should be more vigorous in this process. I am not going to hide the concern that I have, because we are in a new day.

And I believe you mentioned, as I looked at your four elements, we will be writing GAO, because we would like an after-the-fact assessment now that DHS is involved. We would like a more detailed overview of how is it working.

But did I understand that a key enforcement provision was removed which might disallow the president from reopening? Was that your point or could you expand on how we might strengthen—I don't want to undermine the president's role in securing the homeland.

And so if we don't have an enforcement provision, why don't you share with us how we can strengthen that?

Ms. CALVARESI-BARR. Well, I think from some of the cases that we have looked at, as I said, in the past reviews that we had done, we had seen a couple of instances where certain member agencies had asked that language be inserted in the mitigation agreement that said, "If you do not comply with the agreement set forth within, the president has the authority to reopen and re-look under Exxon-Florio," and we saw a number of cases in which that was a debate among CFIUS members.

And in a few cases, allowing that provision in the agreement was struck. It didn't occur. I think we heard today that this is one of the views and certainly the positions that Homeland Security is bringing to the table to say that that helps strengthen and helps keep in place these agreements, the force of compliance with them, and it is a good thing to put in place.

Again, we haven't looked at any new cases since our 2005 work, but I think we heard today that we are seeing more instances in which the reopening of a case is being inserted in those mitigation agreements.

That is something, again, we would have to look at if you asked us to do so.

Ms. JACKSON LEE. Well, I think the point that you are making is through administrative deliberation and shifting, decisions were made to eliminate that provision, which some of us might think that it is minimally a provision that provides the extra enhanced security and as industries and purchasers and others become more

comfortable with our role, I would think that that should not be waived.

And one could say if we are selling candy, what could happen, but I would suggest that the security, again, goes above and alongside of the traversing of commerce.

For that reason, Secretary Baker, let me share with you a point of CFIUS that, frankly, I wonder whether we have considered.

Investment, which, as I indicated to you, which Ms. Clarke has indicated to you, we compete against cities, each other, as to how much investment we can secure.

One of the challenges that has occurred is that our states and local jurisdictions have begun to assess their revenue bases on how much investment they can get in selling off critical infrastructure, to the extent that roads are being sold, happily so.

So if you have an investment that is a lease of 70 years, to my understanding, CFIUS does not assess whether or not that kind of transferring of operation, of control should have a review.

That is investment. That is not acquisition.

Would you care to speculate that it might be valuable to have some standards by which you could review that kind of investment?

Mr. BAKER. I would not necessarily rule out the idea that if the lease was for sufficiently long, that it would be the equivalent of an acquisition. And I agree with you that when roads and other infrastructure are privatized, the nature of the concern about how to protect homeland security changes, because you move from governmental control, which is often very concerned about risks of that sort, to private control, where the concerns are focused on making sure that the quarterly profit projections are met.

And that simply changes the nature of the kinds of measures people are willing to take. I don't know that it is limited to foreign investment. And so one of the questions is, is this a broader question than simply looking at foreign investment?

Ms. JACKSON LEE. Well, clearly, this committee will look at a range of investments and certainly—and when I say that, we will look at critical infrastructure and how it is protected and what kind of security, if you will, plans are in place.

So clearly that can be the case. This obviously is a committee hearing addressing the question of foreign ownership and we are moving forward because our next hearing will also include investment.

But I think you raise a very valuable question and that is the question before this committee.

Let me conclude with Mr. Garcia—thank you, Secretary—to simply let you answer the question I asked Colonel Stephan, how you are coordinating with his discipline and his area under Department of Homeland Security, between the two of you, and particularly as it relates to the question before this committee.

Mr. GARCIA. Exactly as he said. We have important integration with all of the 17 critical infrastructure sector-specific plans.

My organization was responsible for working with the private sector in producing the IT and the communications sector-specific plans, but we, as Secretary Stephan said, have had visibility and input into each of the other SSPs to ensure that there is a con-

sistent level of attention to the cybersecurity dimension of all of the critical infrastructures.

Ms. JACKSON LEE. Thank you very much.

And with that, let me yield to the gentlelady, for 5 minutes, from New York.

Thank you.

Ms. CLARKE. Madam Chair, thank you.

I just wanted to get one more question in here, because this has to be something that I am sure each of you gives some scrutiny to.

Once we enter into these agreements, is there a monitoring process, because you may be talking about an acquisition, you may be talking about a lease, but these are private entities that now have ownership and stake, that would detect corruption?

An individual was now hired as part of this process of maybe managing a port or what have you, that becomes a corruptible element after the transaction has been done.

Is there something that we do through CFIUS or any other means, through the agencies, Mr. Secretary, that would enable us to detect that in any real tangible way?

Mr. BAKER. Yes, there is. We have really pioneered in the use of audits, to go into companies long after they have signed these agreements to say, "Let me see your training. Let me see how you are implementing this. What did you do in this circumstance?"

We have the authority to do background checks on many of the employees or to require that they be done at the company's expense and any adverse information provided to us.

So we actually have built a lot of controls into the follow-on process of making sure people live up to their promises.

Ms. CLARKE. And then, finally, in the initial stage, where you do your 30-day investigation, is that part of the due diligence, as well, in terms of identifying personnel or individuals who may have some shady dealings?

And knowing that it is a 30-day process, with an opportunity to extend to 45 days, do you feel that this is an adequate amount of time for all of the investigations or would you recommend a different timeframe?

Mr. BAKER. Yes. In terms of the timeframe, it often is not enough time. Frequently, it is. Let me first address your first question.

Yes. We ask the intelligence community, and that would include law enforcement, to check or any adverse information on any of the people that are critical to the transaction and when we find adverse action, we will usually try to address it in the mitigation agreement or simply by saying no to the transaction.

In terms of time, it sometimes is not enough. This is why we ask companies to come in early and tell us about the transaction. If they don't, it certainly counts against them, in our estimation, when we are evaluating the 30-day clock.

We can always ask the company to withdraw the petition and to re-file it after we have worked out the issues between us.

We are willing to do that and we have done that fairly often. That gives us the flexibility that we need.

So we have not generally supported extending the deadlines for fear that if you give a government agency 45 days to make a deci-

sion, they will take 44 at least. And so just extending the deadline will delay everyone and we didn't want to do that.

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

Ms. JACKSON LEE. We thank you for your very important contributions.

Let me just close with a question, Mr. Secretary.

I indicated that we were going to ask GAO to do a fresh study, but you noted the very, I think, instructive criticisms or analysis that was already made on the CFIUS process.

Again, I said I am of the position that DHS needs to be more vigorous.

You know, we have heard this massive debate about security, border security. I always believe that what we missed out in 9/11 is that we were not offensive or we were not able to fend off before the terrorists arrived here on this soil.

We can always stand back after they have arrived, maybe we would be even lucky enough to prevent it as they arrive or as they begin to plan.

But wouldn't it be better to be away ahead of the game?

And so the criticisms that have been offered or the analysis that has been offered by GAO I think maybe warrant some legislative fixes.

One of them, however, is an annual report and I would like, for the record, your assessment on that. And you might also give me your assessment on the mitigation aspect, giving the president the continuous authority to reopen, not a waivable authority, which is a decision made by the CFIUS committee, "We will decide to keep it in or we will not."

I, frankly, believe that it should not be left up to chance.

Secretary Baker?

Mr. BAKER. Very good. Let me address the second one first.

On authority to reopen transactions, it has some appeal, I understand, but it would raise real questions among investors about whether, if they made an investment in the United States and the climate changed in 10 years, their deals might be overturned.

We do have the authority, if they lie to us, if they leave out a fact that they know is important to us and they just don't tell us, in the CFIUS process, we can reopen the transaction and we think that gives us a lot of authority, the ability to say "You violated the agreement which led us to approve this deal. So we are reopening" is also one which we use fairly carefully, but which has stood us in good stead on very important transactions.

And so I think the value of a continuing permanent authority to reopen transactions is not offset by the risks to investments.

As far as GAO's report, I thought it was a very thoughtful, detailed report. Many of those recommendations are things that we are now doing one way or the other.

An annual report raises some concerns about confidentiality of these transactions. Investors do not want their deals and the doubts and concerns and negotiations that went into them in the newspapers often.

We would have to be very careful about how a report like that would end up being used. But we are certainly not opposed to giv-

ing this committee as much information about CFIUS as you would like.

Ms. JACKSON LEE. Well, let me thank all of the witnesses. I would simply suggest to you that having been part, in my past life as a lawyer, practicing in a number of areas, been looking over many, many tables with document scattered and wondering whether the deal legally was going to be consummated.

I understand what apprehension these proponents or participants in the transaction may believe, but clarification, protecting the kind of data that would be in the report, I think, frankly, information is a score of points when it comes to protecting the homeland.

And, frankly, I would like to see some way of managing that in a way that does not do damage to the commerce and the comings and goings of business here in the United States.

Again, this hearing started with the premise that if a horrific manmade tragedy were to occur, I think that a combination of Department of Homeland Security and this committee, more than any others, would be asked the question, "Why," and that means it is crucial that we continue to have vigorous oversight.

You have given us this morning a very, very good roadmap to begin this journey of reviewing critical infrastructure across American and foreign ownership and investments, as well as, generally speaking, the critical infrastructure, which, Secretary Baker, you said 80 to 90 percent is in the private sector.

Good news, but yet we have a responsibility to secure the homeland.

I would like to thank the witnesses for their valuable testimony and the members for their questions.

The members of the subcommittee may have additional questions for the witnesses. We will ask you to respond expeditiously in writing to those questions, and we will have several.

And hearing no further business, this committee will stand adjourned.

As I also thank the ranking member, Mr. Lungren, who had another meeting, and the members of this committee for their presence here today in this very important challenge.

Thank you. The meeting is adjourned.

[Whereupon, at 11:49 a.m., the subcommittee was adjourned.]