Statement for the Record

Stewart A. Baker
Assistant Secretary for Policy

Robert B. Stephan
Assistant Secretary for Infrastructure Protection

Gregory Garcia
Assistant Secretary for Cyber Security and Telecommunications

Before the

United States House of Representatives
Committee on Homeland Security
Subcommittee on
Transportation Security and Infrastructure Protection

March 23, 2007

Stewart A. Baker
Assistant Secretary for Policy

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

Robert B. Stephan
Assistant Secretary for Infrastructure Protection

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.

Gregory Garcia
Assistant Secretary for Cyber Security and Telecommunications

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.

.