Testimony of David Marchick[1]

before the

House Committee on Homeland Security
Subcommittee on Transportation Security and Infrastructure Protection

on

"The Impact of Foreign Ownership and Foreign Investment on the Security of Our Nation's Critical Infrastructure"

May 16, 2007

Chairman Jackson-Lee and Ranking Member Lungren:

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

I plan to discuss three issues in my testimony:

> First, the concept of "critical infrastructure" and the implications of foreign ownership thereof;
>
> Second, recent developments in the Committee on Foreign Investment in the United States;
>
> Third, CFIUS-reform legislation moving through the Congress.

Foreign Ownership of Critical Infrastructure

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

---

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

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

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

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

This definition, by setting a high threshold, implies that a relatively narrow list of assets would be deemed to "have a debilitating effect." Core communications assets or the electrical grid certainly would meet this definition. But in the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, the White House identified twelve very broad sectors as critical infrastructure, including agriculture and food, water, and public health.[3] In the book that I co-authored with Monty Graham of the Peterson Institute, Mr. Graham estimated that these twelve sectors cover some 25% of U.S. employment.[4] Taking this effort one step further, the Department of Homeland Security created a "national assets database," which contains tens of thousands of entries compiled from various sources, including state and local officials. The Information Assurance and Infrastructure Protection Division of DHS reported that it had identified 1,700 "critical assets" in 2004. And since 2001, there have been four different executive orders or reports, each of which included *different* sectors as critical infrastructure.[5]

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

---

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

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

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

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

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

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

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

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

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

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

require a national security review simply because, among the many diverse customers of the product, some are located in "critical infrastructure" sectors?

To be sure, the answer to that question may be "yes" in some instances. Moreover, Exon-Florio and the CFIUS process can adequately identify and mitigate risks in those cases. However, even sophisticated counsel frequently have difficulty identifying which instances these concerns may arise, or the potential costs associated with those issues. And this uncertainty is itself very costly, both for U.S. sellers who have an interest in creating the largest possible market for bidding and certainty with respect to closing, and for foreign investors who, in formulating their bid, must assess additional costs associated with their investment and how potential regulatory uncertainty both in timing and result might affect their competitive position vis-à-vis other bidders.

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

Recent Developments in CFIUS

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

- Committing additional resources to staffing CFIUS cases. Treasury has added a new CFIUS Deputy Assistant Secretary and DHS has added case officers and lawyers to focus on reviews and enforcement;

- Involving more senior level officials within CFIUS;

- Enhancing communications with Congress;

- Expanding coordination among intelligence agencies;

- Expanding the use of mitigation agreements and introducing new, tougher terms in such agreements; and,

- Enhancing enforcement of mitigation agreements, including through on-site audits and consultations with parties to such agreements.

In many respects, CFIUS has taken a much more cautious attitude toward their work post-DPW. This caution has had a ripple effect on the private sector, leading to more filings. In 2006, there were 113 filings (up 73 percent over 2005), 7 second-stage investigations (up 250 percent) and 5 withdrawals (up 150 percent) during the second-stage investigation period. A number of other

transactions were withdrawn during the initial 30-day period. The dramatic increase in the number of second-stage investigations and withdrawals suggests that foreign investors are having a more difficult time closing transactions in a timely fashion. The stakes are high – the value of just one-third of the transactions that were submitted to CFIUS exceeded $95.5 billion in 2006.

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

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

Legislative Efforts to Amend Exon-Florio

In the wake of the Dubai Ports World controversy just over a year ago, more than 20 bills were introduced in the House and Senate that would have restricted or blocked foreign investment in one way or another. Certain of these bills would have simply prohibited foreign investment in critical infrastructure; others would have prohibited foreign government ownership of certain assets in the United States. Several bills would have amended Exon-Florio, the statute that gives the President the power to block certain transactions that threaten U.S. national security. One bill amending Exon-Florio passed the House, and another passed the Senate, but the 109th Congress ran out of time before the bills could be reconciled.

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

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

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

- Enhance Congressional oversight and reporting to Congress without politicizing transactions;

- Require higher-level involvement in CFIUS decisions;

- Expand the factors that CFIUS must consider to reflect post-September 11 imperatives, including protection of critical infrastructure;

- Heighten scrutiny for government-owned transactions without impeding investments that don't raise real national security issues; and,

- Allow for transactions to be reopened based on material intentional breaches of mitigation agreements where no other adequate remedy exists. This provision - the so-called "evergreen" provision - is tough medicine and a provision which foreign investors and key elements of the U.S. business community oppose.

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

- Adopts the concept of rotating lead agencies and vests enhanced authority in those agencies to negotiate, monitor and enforce mitigation agreements. For example, DOD would take the lead on defense acquisitions; Homeland Security would lead on investments in ports, airports and transportation companies; Justice would take the lead where law enforcement issues were paramount; and Commerce would take the lead on transactions with significant export control issues;

- Eliminates some of the unnecessary bureaucratic provisions of H.R. 556, such as requiring two-thirds votes in CFIUS for certain decisions. Unlike Congressional committees, agencies don't typically vote; and,

- Imposes the same confidentiality requirements on Congress that exist within CFIUS.

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

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

Conclusion

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

According to the Treasury Department:

- Foreign companies in the U.S. employed more than 5 million U.S. workers in 2005, providing 4.5% of all private sector employment in the United States.

- Manufacturing jobs accounted for 33% of the jobs created by foreign companies in the U.S. (2004 data). The manufacturing sector accounts for just 12% of overall U.S. private sector employment. Thus, FDI is disproportionately bolstering this important sector.

- An additional 4.6 million U.S. jobs indirectly depend on foreign investment in the U.S. (2005 data). Foreign companies in the U.S. buy 80% of their inputs from U.S. companies. This additional business indirectly supports almost as many U.S. jobs as FDI creates directly.

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

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

We need more foreign investment, not less.

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

Thank you for the opportunity to testify before your committee.