SHEILA JACKSON LEE
18TH DISTRICT, TEXAS

WASHINGTON OFFICE:
2435 Rayburn House Office Building
Washington, DC 20515
(202) 225-3816

DISTRICT OFFICE:
1919 SMITH STREET, SUITE 1180
THE GEORGE "MICKEY" LELAND FEDERAL BUILDING
HOUSTON, TX 77002
(713) 655-0050

ACRES HOME OFFICE:
6719 WEST MONTGOMERY, SUITE 204
HOUSTON, TX 77019
(713) 691-4882

HEIGHTS OFFICE:
420 WEST 19TH STREET
HOUSTON, TX 77008
(713) 961-4070

FIFTH WARD OFFICE:
3300 LYONS AVENUE, SUITE 301
HOUSTON, TX 77020

Congress of the United States
House of Representatives
Washington, DC 20515

COMMITTEES:
JUDICIARY
SUBCOMMITTEES:
COURTS, THE INTERNET, AND INTELLECTUAL PROPERTY
IMMIGRATION, CITIZENSHIP, REFUGEES, BORDER SECURITY, AND INTERNATIONAL LAW
CRIME, TERRORISM AND HOMELAND SECURITY

HOMELAND SECURITY
SUBCOMMITTEES:
CHAIR
TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION
BORDER, MARITIME, AND GLOBAL COUNTERTERRORISM

FOREIGN AFFAIRS
SUBCOMMITTEES:
AFRICA AND GLOBAL HEALTH
MIDDLE EAST AND SOUTH ASIA

SENIOR WHIP
DEMOCRATIC CAUCUS
WHIP
CONGRESSIONAL BLACK CAUCUS
CHAIR
CONGRESSIONAL CHILDREN'S CAUCUS

CHAIRWOMAN SHEILA JACKSON LEE, OF TEXAS

HEARING ON:

"ENHANCING AND IMPLEMENTING THE CYBERSECURITY ELEMENTS OF THE SECTOR SPECIFIC PLANS"

OCTOBER 31, 2007
311 CANNON

I would like to take this opportunity to thank all of you for joining us this afternoon to discuss the urgent topic of private sector participation in protecting our country's critical infrastructure. I am particularly grateful to Chairman Langevin for inviting the Subcommittee on Transportation Security and Infrastructure Protection to participate in this hearing, and I look forward to future collaboration where our issues of concern intersect.

Today's hearing regards the implementation—or existence—of the cyber security elements of the 17 Sector Specific Plans (SSPs) under the National Infrastructure Protection Plan (NIPP). Ranking Member Lungren and I take particular interest in this topic as DHS' infrastructure protection efforts fall under our subcommittee's jurisdiction. We have been—and continue to be—very vigilant about the Department's protection of our nation's critical infrastructure beyond cyber security, to also address physical and human considerations.

Thanks to Chairman Langevin, however, we will learn today about how the Department is protecting critical infrastructure from a cybersecurity perspective, and I look forward to seeing

how the lessons learned today apply to other critical infrastructure protection (CIP) programs. Thus far, I have not been very impressed with DHS' CIP efforts.

CIP is a massive and unprecedented undertaking. According to the Homeland Security Act of 2002, "critical infrastructure" includes "systems 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 these matters." Based upon this definition, "critical infrastructure" is not just bridges and water utilities, but also financial centers and transactions. It is, therefore, clear that when such a vast and important mission is combined with a young agency, it is incumbent upon it and its oversight committee to have frank and honest discussions about the efficacy of our CIP efforts.

Protecting these systems and assets from natural- and human-made disasters is exacerbated by the fact that approximately 85 percent of the country's critical infrastructure is owned and operated by the private sector. Furthermore, this Administration did not encourage the government to regulate and mandate private sector owners and operators protect their critical infrastructure but, instead, it encouraged voluntary partnerships. How well the Department manages this voluntary relationship with the private sector to protect our critical infrastructure is—and will continue to be—a major priority for our Committee, and my subcommittee specifically.

Recently, Chairman Thompson and I directed Committee staff to investigate the implementation of the NIPP and SSPs to learn whether they are motivating private industry to protect our critical infrastructure. Because such a large task is based upon a voluntary partnership, we need to give great attention to whether actions are, indeed, being taken. That will be the focus of my attention at today's hearing.

The release of the NIPP and the SSPs was delayed significantly. Unfortunately, the threat to our critical infrastructure was not simultaneously delayed. As a result, we have to quickly determine whether these plans are being implemented by owners and operators to better protect our critical infrastructure. It is not enough to create large, nearly unreadable documents and to discuss processes; instead, we must focus on implementation and execution. For instance, we must have effective and efficient communication between private sector owners and operators of critical infrastructure and all levels of government.

On September 26, 2007, Chairman Thompson and I sent a letter to Assistant Secretary Stephan and Director Caverly about the implementation of the SSPs and the status of the National Annual Report that is supposed to describe the implementation of protection efforts. Based upon the Department's responses, we are quite concerned about whether verifiable action is being taken by the private sector.

I am not here to reprimand the private sector or to viscerally call for its regulation. Because of the mission, however, I believe that all options should be on the table. I believe that we need to give these partnerships a chance. We need to know whether the Department is executing them effectively. I believe the owners and operators of these assets will, in most cases, act without regulation if an effective case for action is made and there is adequate and necessary follow through by the Department. I want to learn from our witnesses from the private sector how the Department can be more effective in encouraging this necessary—and urgent—activity.

It is now time for an open and honest conversation about protecting our critical infrastructure. We are done with documents and verbiage. It is time for action. It is time for us to learn about the tools you need and how this Congress can help. We may not need a regulatory hammer, but we certainly need a national discussion about civic and corporate responsibility. Perhaps today's hearing begins that conversation and will lead to concrete steps that will make America truly safer.