Testimony of Michael Pfister
Halliburton Senior Vice President and Chief Information Officer
Before the U.S. House of Representatives
Committee on Homeland Security
16 May, 2007

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

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

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

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

Halliburton operates industry - standard firewalls, antivirus, and intrusion prevention systems to separate our internal network from the Internet. Halliburton performs perimeter audits to ensure the firewalls are doing their jobs. We regularly monitor for suspicious activity and isolate that activity before it can do any harm. We utilize third party security experts to test our security

system's effectiveness. We encrypt digital communications before transporting them through public communications networks.

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

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

- Halliburton facilities have physical barriers (fencing, locked doors, and locked traffic gates) and security guards to prevent unauthorized entry and access to both tangible and intangible property.

- Halliburton restricts access to facilities to persons having proper credentials, such as electronic badges. Badge access records are automatically made and maintained.

- Visitors to Halliburton facilities are required to sign-in and then are escorted throughout the facility.

- Halliburton marks certain documents as "confidential" or uses other appropriate headers / legends when such documents contain confidential information of the company.

- Warning labels appear on computer log-in screens to inform users that the system contains business confidential information and is for company use.

- Halliburton stores trade secret information (drawings, specifications, etc.) in an electronic vault that is referred to as the Matrix database. To control access to the trade secret information, the Matrix database recognizes the degree of authorization that has been granted to a user and appropriately limits the user's access to authorized data in the system.

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

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

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

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

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

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

In addition, when Halliburton engages a third party to provide goods or services and Halliburton is required to disclose confidential information to the third party, the third party is contractually obligated to maintain the confidentiality of such information. Typically, when a third party is engaged in Halliburton technology development, all rights to the developed technology are assigned to Halliburton, and again, the third party is required to maintain the confidentiality of Halliburton's proprietary information. In some cases, the developed technology could be jointly owned by Halliburton and a co-developer, but in those cases as well, the parties will be obligated to maintain the confidentiality of proprietary information shared by one with the other.

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

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