Testimony of

Richard E. Hovel
Senior Aviation & Homeland Security Advisor
The Boeing Company

Before the House Homeland Security Committee
Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment

May 25, 2007

Since the tragic events of September 11, 2001, and consistent with **HSPD-5**, the **National Response Plan**, **National Infrastructure Protection Plan** and the **National Intelligence Strategy**, there have been increasing strides made to integrate the private sector within the public sector information sharing framework throughout all levels of government.

With approximately 87 percent of this nation's critical infrastructure residing within the private sector, one can hardly expect public sector law enforcement and intelligence entities to sufficiently insulate industry from risk associated with what was once [primarily] "criminal enterprise". Understanding and responding to the many inter-dependencies between the various elements of the critical infrastructure may be more appropriately and effectively addressed by private sector ownership, with support from public sector agencies. This is based upon a sound pro-active understanding of the far-reaching damage that a successful attack on critical infrastructure could have – and is somewhat contrary to the largely reactive nature of traditional law enforcement.

Because of this, information that is developed regionally may have significant impact nationally. This was evidenced by the recently thwarted terror plot at Fort Dix. To be effective in this arena, industry must have real-time access to information through Fusion Center capabilities, in order to analyze that which may have a local or broader impact. Conversely, federal, state and local government, law enforcement and intelligence entities must have access to mature intelligence capabilities in the private sector.

The private sector has the ability to effectively acquire, interpret, analyze and disseminate intelligence information – which may originate from private sector sources. In deed, many companies are authorized to receive, store and communicate classified information by employees already holding clearances. Public/private sharing of intelligence information is a function of "trust" and as we well know, "all trust is local" which provides the very foundation for the Fusion Center concept.

Capitalizing on the already significant relationships that exist between the public and private sectors in the Northwest and to mitigate ever-changing risk, Boeing is in the process of assigning an analyst to the Seattle FBI Fusion Center. Fortunately, the federal

government has put in place a mechanism which enables private industry to enter into such collaboration, namely, the federal SAFETY Act ("Support Anti-terrorism by Fostering Effective Technologies Act of 2002.") Boeing is currently working with the Department of Homeland Security in an effort to submit an application for protection under the SAFETY Act. Hopefully, this will be the first of many similar efforts across the nation that will establish a collaborative partnership between the public sector and industry, and protect our critical infrastructure more effectively and expeditiously.

A communication hub, around which the fusion concept could be built would use the collaborative efforts of both the private and public sectors, working in conjunction with the Pacific NW Economic Region (PNWER) Center for Regional Disaster Resilience have formed the community-focused Northwest Warning and Response Network (NW WARN). While the genesis of this was based upon the Emergency Response Network (ERN) model implemented in the Southwest, NW WARN is a much more robust "all hazards – all threats" communication tool. This network provides multi-directional communications between the FBI and both public and private interests across the five Northwestern-most States of Alaska, Montana, Idaho, Washington and Oregon.

Additionally, we are in the formative stages of establishing a virtual Regional Information Fusion Center Pilot Project (RIFCPP) that would provide two-way information sharing based on a multi-layered secure and resilient system with analysis produced by a team of core resident local and state experts with virtual analysts from different sectors and disciplines. They would be using a largely virtual database to enable integration, assessment, and secure, tailored dissemination of information provided to key stakeholders.

This analysis would be used for organizational and collective decision-making and crafting public information. This virtual capability will interconnect state, local, private sector, defense and other stakeholder capabilities while avoiding duplication of effort, proliferation of analytical products, and competition for hard-to-find analytical staff resources. It will also enable federal authorities to have a single focal point to efficiently and securely provide intelligence and other sensitive information to a wide range of customers. This pilot would provide a model which could be customized by states and localities across the nation.

The overarching purpose of these collective efforts is to better identify infrastructure interdependencies and preparedness gaps. They focus emphasis on identifying asset criticality, managing disasters and furthering the "trust-factor" between key stakeholders while moving the law enforcement and intelligence communities beyond the **"need to share"** philosophy toward a **"responsibility to provide"** model.

Thank you for your time and support in finding solutions to take advantage of both public and private sector capabilities.