

# Executive Summary

On November 29-30, 2005, the Center for US-Japan Studies and Cooperation of Vanderbilt University hosted the second annual US-Japan Critical Infrastructure Protection Forum (US-Japan CIP Forum). This event was intended to continue an important dialogue that began in 2004 between US and Japanese industries over how to safeguard critical assets from harm. As the 2005 Forum was organized in close coordination with the US Department of State and the Japanese Embassy in Washington DC, which were both involved in planning the US-Japan bilateral talks on cyber security, the event enjoyed a significant increase in participation from US and Japanese experts in the field.

To maximize some of the important lessons learned from the inaugural US-Japan CIP Forum 2004, which focused on identification of common physical and cyber security issues and solutions across multiple sectors, the US-Japan CIP Forum 2005 agenda endeavored to examine some of the important cooperative relationships between and among public and private sectors that support CIP activities.

Over 70 individuals representing 48 organizations from the US and Japanese governments and industry met for a day and a half to address the importance of cross-agency, cross-sector and cross-national communication, cooperation and coordination in all aspects of physical and cyber infrastructure activities, including preplanning, response, recovery and reconstitution, in an increasingly interconnected global economy.

## *The Agenda*

- To kick off the event, Mr. Yoshiyuki Kasai, Chairman of the Central Japan Railway Company (JR Central) described some of the measures his company has taken—in light of recent terrorist attacks on passenger railways systems (Madrid in 2004 and London in 2005) —to safeguard the Tokaido Shinkansen (also known to many in the US as the “bullet train”) from attacks. Mr. Kasai was followed by two US government (USG) officials who spoke on the immense destruction and devastation caused by Hurricane Katrina and Hurricane Rita, and the response and recovery efforts undertaken by federal, state, and local governments and the private sector.

- The Forum then proceeded with presentations that dealt with the main theme of the conference: the importance of partnership in CIP, including critical information infrastructure protection (CIIP). Two speakers, each representing the US and Japanese perspective, addressed some of the mechanisms that have been established in the US and Japan to improve government-industry, industry-industry CIP and CIIP coordination, as well as some of the impediments to improved information sharing and cooperation.
- The first day of the conference concluded with two presentations that addressed the growing importance of cyber security in CIP activities. The two presenters arrived at similar a conclusion (independently of each other): the global nature of the information infrastructure demands an international approach and solution to cyber security. To this end, both presenters called for the creation of an international center to help coordinate and facilitate cooperation on information security issues for the international community.
- The second day of the conference was dedicated to understanding critical infrastructure interdependencies. To demonstrate the interrelations between critical infrastructure companies in the US and Japan, the US-Japan CIP Forum 2005 dedicated half a day to conduct a tabletop exercise that invited five critical infrastructure industries—electric power, communications, information technology, passenger rail and financial services—to discuss how a single event, a blackout lasting for three to four days, would impact their operation, and what emergency response plans would be implemented.

### *Lessons Learned*

- One of the greatest challenges to CIP and CIIP is the involvement of multiple players that have different missions, goals and objectives and play by divergent rules.
- Critical infrastructures in the US and Japan are interlinked and interdependent on a national and global scale.
- CIP and CIIP issues cannot be resolved domestically; they demand an international approach with international solutions.

- Complete (with no TBDs or “to-be-done” items) emergency response plans for physical and cyber infrastructure disruptions must be prepared in advance and regularly tested for “kinks.”
- Emerging technologies will not only replace systems and change the way business is conducted, but will also increase vulnerability by changing the nature of risks and threats.
- It is important to prioritize CIP and CIIP activities as public and private resources are always limited.

### *Going Forward*

- A “culture of security” and a “culture of information sharing” must be established worldwide to better protect critical physical and cyber infrastructure.
- More risk and vulnerability assessments need to be conducted by governments and industries, which must then be integrated so that practical and reasonable CIP and CIIP policies can be developed.
- An international discussion on the legal framework of CIP and CIIP must take place.
- Industry must educate lawmakers and decision makers on physical and cyber infrastructure protection issues so that they can deliberate more intelligently on drafting security legislation.