



Fourth U.S.-Japan Critical Infrastructure Protection Forum

*Vanderbilt Institute for Public Policy, Center for
U.S.-Japan Studies and Cooperation*

Tokyo, Japan

November 28-29, 2007

Distribution of this report is restricted to the attendees of this conference only. Consent from the organizing committee is required should a recipient of this conference wish to use any material contained in this report.

Table Of Contents

Introduction	1
Executive Summary	3
Presentations	6
Session Number 1: The Earthquake and Kashiwazaki-Kariwa Nuclear Power Station	
Mr. KOMORI, Akio	
TEPCO's Kashiwazaki-Kariwa Nuclear Power Plant	6
Mr. YAMADA, Tomoho	
Actions Taken by Nuclear and Industrial Safety Agency (NISA)	8
Mr. Richard McPherson	
Lessons Learned of Earthquakes and Nuclear Power Safety	12
Session Number 2: Best Practices and Constructive Approaches for Planning and Executing Compliance Management	
Mr. Scott Smith	
Comprehensive Approaches	13
Mr. TAKAHASHI, Masakazu	
Information Technology and Computer Security	15
Mr. KITAGUCHI, Takaya	
Niigataken Chuetsu-Oki Earthquake: NTT Response and Lessons Learned	16
Rear Admiral James Kelly; Commander, U.S. Naval Forces, Japan	17
US-Japan Cooperation for Disaster Relief	
Session Number 3: National Cyber Attack/Cyber Crime and Countermeasures	
Mr. ISHIKAWA, Shoichiro	
Cyber-crime and Cyber-terrorism Countermeasures; Security Measures for the G8 Hokkaido Toyako Summit	19
Mr. Phil Sodoma	
Preparation for National Level Cyber-crime/Cyber-Terrorism	21
Mr. Richard McPherson	
Nuclear Safety and U.S. Navy Nuclear Power	23
Keynote Speaker – MR. HASHIMOTO, Shin	
Executive Vice President NTT Corporation	
NTT's Vision for Communication Infrastructure Protection	25

Major General James Flock; Deputy Commander, U.S. Forces, Japan. Evening Speaker: Disaster Relief Operations in Japan and USFJ	27
Session Number 4: “Is Minneapolis the Tip of an Iceberg? Concern for Physical Aspects of Aging Structures” Dr. Michael Leineweber; Durant Media Five	28
Mr. NISHIKAWA, Kazuhiro The Fear of Aged and Damaged Critical Infrastructure	30
Mr. TAKAGI, Sentaro Changeover to a Preventive Maintenance Type Control in the Tokyo Metropolitan Government	31
Keynote Speaker: Governor ISHIHARA, Shintaro	32
Roger Mall; Microsoft Corporation, Virtual Earth Business Development Manager Imagery and Critical Infrastructure Protection How Governments and Companies Are Using Imagery to Manage Risks, Enhance Operations, and Respond to Emergencies	33
Session Number 5: Panel on CIP Implementation, Accomplishments and Goals in Japan Mr. YAMAGUCHI, Suguru Work of the National Information Security Center	35
Mr. YOSHIDA, Teruyoshi Security Controls for the Financial Industry	36
Mr. ARIMURA, Koichi Topics form Telecom-ISAC Japan	37
Ms. ITO, Yurie; JPCERT/CC CIIP efforts: Watch and Warning	37
Closing Session	38
List of Participants	39

U.S.-JAPAN CRITICAL INFRASTRUCTURE PROTECTION FORUM
November 28-29, 2007
Tokyo, Japan
Introduction

This report summarizes the conduct of the Fourth Annual Critical Infrastructure Protection Forum hosted by Vanderbilt Institute for Public Policy, Center for U.S.-Japan Studies and Cooperation Director Dr. Jim Auer. This conference—held November 28 and 29, 2007 in Tokyo, Japan—assembled specialists in telecommunications, nuclear power, urban civil engineering, highway maintenance, cyber technologies, military planning, and government policymaking. Participants came from both government and industry backgrounds, and positions. Moreover, they were all specialists representing the two most technologically and economically advanced countries of the world: the United States and Japan.

This conference afforded these specialists with a venue to exchange frankly perspectives on challenges, lessons learned, emerging technologies and concepts, and visions related to critical infrastructure protection. Presentations and discussions centered on five panels and four keynote speakers. The panels consisted of:

1. Actions taken at the Kashiwasaki-Kariwa Nuclear Power Plant in the aftermath of the Niigata-ken Chuetsu-oki Earthquake on July 16, 2007;
2. Best Practices and Constructive Approaches for Planning and Executing Compliance Management;
3. National Cyber Attack/Cyber Crime and Countermeasures;
4. Minneapolis the Tip of an Iceberg? Concern for Physical Aspects of Aging Structures;
5. CIP Implementation, Accomplishments and Goals in Japan

In addition to the five panels above, two keynote and three supporting speeches addressed specific technical aspects of critical infrastructure protection. These five sessions were:

1. Keynote: MR. HASHIMOTO, Shin; Executive Vice President NTT Corporation; Member of the Board, and Director of Next Generation Office: NTT's Vision for Communication Infrastructure Protection
2. Keynote: Governor ISHIHARA, Shintaro: Challenges to Political Leadership in Emergency Reponse
3. RADM James Kelly, Commander, U.S. Naval Forces, Japan: U.S.-Japan cooperation for disaster relief
4. Mr. Richard McPherson, Vice President, DownRange Global Solutions: Nuclear Safety and U.S. Navy Nuclear Power
5. Mr. Roger Mall; Microsoft Corporation, Virtual Earth Business Development Manager Imagery and Critical Infrastructure Protection: How Governments and Companies Are Using Imagery to Manage Risks, Enhance Operations, and Respond to Emergencies

Fourth U.S.-Japan Critical Infrastructure Protection Forum

Although this is the fourth conference in this series, it is the first session convened in Tokyo. This was made possible with the support of many individuals and organizations. The U.S. Embassy supported this conference by allowing the use of its Tokyo American Center; the organizers of this conference are grateful to the Tokyo American Center Director Jeff Jamison and the Center's staff for their kindness and support for this effort. NTT, JR Tokai, Mitsubishi Corporation, Microsoft and CWell LLC made financial contributions that made this frank and mutually beneficial exchange between U.S. and Japan possible.

EXECUTIVE SUMMARY

This fourth annual Critical Infrastructure Protection (CIP) Forum focused on disaster response at the Kashiwazaki-Kariwa Nuclear Power Plant; nuclear safety; cyber-crime and cyber-terrorism; telecommunication threats and security; dangers and management of aging bridge structures; and Japan's organizations to develop partnerships for CIP among governments, industries, and research centers.

Presentations and discussions identified several concepts and lessons learned common to various infrastructure sectors. Points overlapping sectors included the following:

- In the scheme of successful plans, response, and recovery for infrastructure protections government and industry cooperation is essential. In this regard, all entities involved should seek public views and concerns. Furthermore, in most cases the infrastructure to be protected belongs to a private entity; however, authorities, coordination, and assets for response often belong to governments from the local through national levels.
- Critical infrastructure sectors are a cross section of various systems; as various CIP sectors develop, systems increasingly become integrated. As an example telecommunication systems are dependent on power systems, financial systems intersect with cyber systems, and disaster response to a collapsed bridge keenly are dependent on communication systems.
- Maintaining a constant and rapid flow of communications with governments, within industries, and the public during emergency situations is a high priority in preserving safety, and efficiently responding to urgent situations. Entities with 24/7 command and control elements have been able to respond more rapidly to mitigate damage and recover services.
- Infrastructure sectors should integrate training and exercises for sustained operations and in preparation to respond to urgent situations. In this regard, individuals should be trained at every level, and not rely on a hierarchical flow of information to direct responses.
- Preparations to respond to future challenges typically are based on yesterday's problems; however, we should recognize that events of scale are unpredictable. We should therefore consider contingencies beyond what we have already experienced, and the events that may occur unexpectedly.

Sector specific concepts and lessons-

Bridge infrastructures:

- Though there were many technical inspections of the Minnesota bridge, there was no political response to these reports. Political involvement and decisions are an essential element to maintaining and rebuilding infrastructure.
- First responders able to act swiftly will save more lives.
- The Minneapolis bridge collapse was of a State bridge, over a county river, between two banks of a city. All had communications within 15 minutes of the collapse. Complications were overcome before the disaster occurred because of planning, training, and exercises.
- Inspection of concrete bridge portions should not be limited to exterior observations. Internal steel supports can deteriorate despite being covered by paint or concrete.

Nuclear Power:

- Nuclear power has over 10,000 years of operations; of these 10,000 year of operation, the U.S. Navy has 5,800 reactor years of safe operations, over half of the world's total without a failure. Navy nuclear power has safely steamed over 135 million miles and is welcomed at 150 ports around the globe in 50 countries. These are the results of a nuclear power program that have emphasized processes of selection, education, testing, surveillance, and implementation of lessons learned.
- Nuclear power facilities should have on site its own fire fighting capabilities, and not rely on local communities for assets to respond to emergencies.
- Government and industry must maintain the flow of information during and after an emergency. Additionally, they must seek various methods of disseminating information to the domestic public, and in international affairs with other governments.
- Gathering lessons learned and disseminating this information to the nuclear power community over 50 years is the fundamental reason for successes in nuclear power safety. Every year nuclear power becomes safer because of this.

Cyber-crime and information technologies:

- Threats to IT and computing are changing in sophistication, motivation, and severity. Early threats to computers required relatively unsophisticated skills to cause mischief motivated by curiosity or entertainment. The fastest growing segment of threats to networks now is from highly skilled individuals posing the most severe and costly types of threats.

Telecommunications:

- To reduce transmissions during a surge yet facilitate personal messages during an emergency situation, NTT established a "Disaster Emergency Message Dial" service operated within a town network. The service conveys messages notifying friends and relatives that the individual/family is safe, and location to which they moved as a result of a disaster. A "Disaster Message Board" Service was created for PC or cell phone users to place similar information on internet based message boards.

- Telecommunication transmissions will surge during an emergency and managing traffic will become an urgent task to ensure that those responding and mitigating damage can communicate. During the 1995 Hanshin 300,000 subscribers lost service while the surge of telecommunications traffic rose 50 times normal levels. During the 2003 Sendai earthquake, NTT DoCoMo cellular traffic rose 20 times normal traffic levels.
- Telecommunications is becoming more integrated with internet protocols. By 2010 the telecommunications industry estimates that 20 million subscribers will be on broadband network-based systems. Telecommunications and cyber systems must manage communications traffic during emergencies while protecting identities and privacy as this integration moves forward.
- The 2004 earthquake in Niigata-ken compelled three types of responses for telecommunication companies. There areas related to facility damage, power outage, and management of communications traffic in the aftermath of the natural disaster. As a result, facilities should be built with greater resilience to shock; contingencies should include alternate power sources (batteries, portable generators); managing telecommunications should prioritize traffic to responders and key emergency entities (911 in US/110 and 119 in Japan). In this regard, VOIP will be a challenge as it will require its own mechanisms to manage information flows.

U.S.-JAPAN CRITICAL INFRASTRUCTURE PROTECTION FORUM
November 28-29, 2007
Tokyo, Japan

Summary of Presentations

Session Number 1: Panel on The Earthquake and Kashiwazaki-Kariwa Nuclear Power Station

Presented by:

-Mr. KOMORI, Akio; Executive Officer and General Manager, Nuclear Quality and Safety Management Office, Tokyo Electric Power Company (TEPCO)

Effects of the Earthquake on the Kashiwazaki-Kariwa Nuclear Power Station

-Mr. YAMADA, Tomoho; Nuclear and Industrial Safety Agency (NISA), Ministry of Economy, Trade, and Industry

-Mr. Richard McPherson; Executive Vice President, DownRange Global Solutions

Presenters during this session provided information from the perspective of the Kashiwazaki-Kariwa Nuclear Power Plant management and operations, the Government of Japan's Ministry of Economic Trade and Industry's, Nuclear and Industrial Safety Agency, and a broad perspective of lessons learned and applied regarding nuclear power safety. These perspectives are summarized in the paragraphs below.

Mr. KOMORI, Akio: Tokyo Electric Power Company's Kashiwazaki-Kariwa Nuclear Power Plant

TEPCO has a total capacity to produce 62 GW of electricity. Each year TEPCO provides the Tokyo metropolitan area with 287 billion kilowatt hours of electricity, one-third of the total Japanese demand for electricity. TEPCO's three nuclear power generating facilities comprise 40 percent of its power. Of these, the Kashiwazaki-Kariwa nuclear power plant is approximately 200 kilometers north of Tokyo and is comprised of seven reactors capable of producing 8.21 GW output; it is the largest nuclear power plant in the world.

The Niigata-ken Chuetsu-oki earthquake struck on July 16, 2007 at 10:13 AM—on a national holiday—registering a magnitude of 6.8 on the Richter scale. Depth of the earthquake was 17 kilometers with the epicenter 16 kilometers from the power plant.

Response to the July 16 Earthquake - Actions taken by TEPCO, METI, and NISA immediately after the earthquake are summarized in the paragraphs below.

Immediate actions taken by TEPCO on-duty operators at the site began within minutes

after tremors stopped. Plant operations initiated a walk down inspection of the facility by 1030 that continued until 1915 the next day. Reporting lines took two paths, one to the various levels of government (village, city, prefecture, and central governments), with the initial report sent at 10:25 to the GOJ, to Kariwa Village at 11:18. The other reporting line was to the public and TEPCO held briefings to the media with four press conferences on the first day, the first of which was held at 10:45.

TEPCO's staff on-site established a temporary operations center by 10:45. Access to its planned emergency headquarters facility—equipped with appropriate contingency communications—was obstructed in the immediate aftermath of the earthquake, and became accessible by 1305 that afternoon.

TEPCO's Kashiwazaki-Kariwa Nuclear Power Plant



In the immediate aftermath of tremors, the reactors' automated safety functions to shutdown, cool, and contain activities operated as designed. Off-site power was maintained through transmission lines. A short-circuit sparked an electrical fire in one of the house transformers (Unit 3), and there were two radioactive leaks from Units 6 and 7 which were found to be well below danger levels to people and the environment in general. TEPCO reporting in the aftermath of seismic activity was done in accordance to established national guidelines that categorize damages to structures, systems and components (SSC), with "Category A" the damages—those raising a safety concerns, such as damages related to reactor pressure, primary containment, and control rods—being the most serious. Inspections found no "Category A" damage; however there were findings of minor cases of lesser categories.

TEPCO continues to inspect its facilities and survey adjacent areas to ensure safety before restarting operations and evaluation of seismic acceleration of its SSC are ongoing. Designed to sustain functions and capabilities up to a 6.5 level earthquake, the effects of the Niigata-ken Chuetsu oki earthquake reached 6.8 on the Richter scale. Although facility appears to have sustained its functions and capabilities despite the earthquake, TEPCO is conducting seismic studies of the land and sea areas surrounding the facility. TEPCO completed survey of the maritime areas around the facility in November, and analysis is ongoing. TEPCO is also conducting land and sea surveys of its Fukushima plant. It is taking

actions to improve its fire-fighting capabilities within the facility, and to improve its communications systems based on lessons learned. Details of lessons learned are reported to the GOJ, and are also available on the TEPCO website¹ in an effort to broadly share lessons learned with the public and industry.

Mr. YAMADA, Tomoho: Actions Taken by Nuclear and Industrial Safety Agency (NISA), Ministry of Economy, Trade, and Industry

The Ministry of Economy, Trade and Industry (METI) and its Nuclear and Industrial Safety Administration (NISA) outlined five areas in response to the July 16 earthquake: Response on the day of the earthquake, On-the-Spot Investigation, public relations, international relations, and actions currently in place.

Day of Earthquake - Immediately after the earthquake, NISA and METI both established respective headquarters to manage operations. The headquarters formed by METI was headed by the Minister himself.

At the same time, actions were taken to analyze data to determine the levels of safety and security at the facility. NISA directed Tokyo Power and Electric Company (TEPCO) to analyze its recorded seismic data for any activity that may have exceeded the facilities' design specifications. METI then directed three actions to be taken at the site. Of these directives, METI also directed other companies operating nuclear facilities to conduct the first two measures below:

- An analysis Kashiwazaki-Kariwa's capabilities to respond to fires at the facility, and to determine any shortfalls;
- An analysis of radioactive material released from the facility; and
- Suspension of the plant's operations until safe operations can be confirmed.

On the Spot Investigation – Nuclear safety inspectors from Kashiwazaki-Kariwa immediately began inspections, and NISA dispatched their Director of Nuclear Emergency Preparedness Division. NISA dispatched an additional team of four to augment investigations headed by the Deputy Director General of NISA to the nuclear power plants at Kashiwazaki-Kariwa. NISA's Director General met with the Mayor of Kashiwazaki City and chief representative of Kariwa village on July 23d to brief them both of actions taken in response to the earthquake, and to conduct on-the-spot investigations of the nuclear power plants there. This was followed up by NISA's Deputy Director General return to the area on July 15th for further investigation of the site.

Public Affairs – METI realized the importance of keeping the Japanese public informed, both at the local and national level, and took several measures to disseminate as the situation

¹<http://www.tepco.co.jp/en/index-e.html>

developed. Press conferences and briefings were held at NISA's headquarters in Tokyo from July 16. They augmented this effort with daily briefs at the off-site emergency center in Kashiwazaki City from July 24th until August 10th. In addition to briefings at these two sites, NISA provided a briefing to citizens at Kariwa village on July 25th, and citizens of the larger Kashiwazaki-Kariwa area on August 1st at Kashiwazaki City. To further disseminate information, METI—in the name of the Minister, Governor of Niigata Prefecture, and Mayor of Kashiwazaki City—arranged for paid space in national papers on July 31st, and in local newspapers on August 1st, 24th, and 30th; and furthermore NISA published and mailed its own information magazine in July, August and September.

International Affairs – The mainstay of actions taken by METI in the aftermath of the earthquake took place with international media, foreign governments, and the International Atomic Energy Agency (IAEA). Only July 18 and 17 NISA briefed the foreign media on the earthquake's effects on Kashiwazaki-Kariwa's nuclear power plants, and the actions taken to date.

Japan's Ministry of Foreign Affairs (MOFA) transmitted instructions to their Embassies to provide official explanations of developments at Kashiwazaki-Kariwa to their host nation central governments.

The Government of Japan received an IAEA proposal to dispatch an IAEA team to Niigata for joint observation with NISA. The proposal was received on July 19, and the GOJ accepted four days later; joint observation of the site was conducted from August 6 through the 10th by the international team comprised of representatives from Sweden, Turkey, the US and Bulgaria and headed by IAEA, Nuclear Installation Safety Division Director Philippe Jamet. They published the mission's published on August 18th noting that the “dose caused by the leak of radioactive materials were well below the regulatory limits” though they also recommended that the plant not be reopened until further tests were concluded. Further details of their findings are as follows:²

- The “automatic shut-down” feature of all the reactors which were at full power or increasing power performed without problems and the installation functioned in a satisfactory manner during and after the earthquake
- The three fundamental safety functions of (a) reactivity control, (b) removal of heat from the core and (c) confinement of radioactive materials were ensured with the exception of very minor radioactive releases which occurred shortly after the earthquake. The radioactive releases to the environment were estimated to result in an individual dose well below the authorized limits established by the regulatory authority for exposure of the public for normal operating conditions.
- Based on the reports from TEPCO experts and the limited in-plant walk-downs and visual observations performed by IAEA experts, safety related structures, systems and

²IAEA, Engineering Safety Review Services Seismic Safety Expert Mission, “Preliminary Findings and Lessons Learned from the 16 July 2007 Earthquake at Kashiwazaki-Kariwa NPP” Report to the Government of Japan 6-10 August 2007, <http://www.iae.org/NewsCenter/News/PDF/kashiwazaki060807.pdf>

components of the plant seem to be in a general condition much better than expected for such a strong earthquake, with no visible damage. This is probably due to the conservatisms introduced at different stages of the design process. The combined effects of these conservatisms were apparently sufficient to compensate for uncertainties in the data available and the methods applied at the time of the design of the plant, which led to the underestimation of the original design basis ground motions.

- In accordance with the new seismic guidelines of the Nuclear Safety Commission (NSC) (issued in September 2006) a re-evaluation of the seismic safety needs to be done taking into account the effects of the Niigataken Chuetsu-Oki earthquake. Any re-evaluation of the seismic safety of the plant, including possible upgrades, requires the input from a new seismic hazard evaluation, seismic analysis and comparison of results with the original seismic design, including also the need to address the issue of the potential existence of active faults underneath the site.
- Further and thorough inspections and evaluations of all critical structures, systems and components of the seven units have not been completed and important components like the reactor vessels, the core internals and the fuel elements have not yet been examined. TEPCO is accomplishing what is to be the first stage of a more comprehensive inspection plan, namely visual observations. Presently, detailed checks of the integrity and operability of all safety systems and components of the frontline and supporting safety related systems are ongoing even though no apparent damage has been sustained. All these activities should be thoroughly and fully documented.
- Consider the possibility that a component remains functionally available under normal operating conditions but sustains hidden damage. This could affect the capability of the component to function as required during potential accidents and its safe long term operation. Therefore, the potential interaction between large seismic events and full functionality also under accident conditions should be analyzed and inspected prior to restart of the plant, and accelerated ageing may be an important topic to consider in future inspection programs.

The report identified specific areas for work, such as fire safety, soil failure, anchorage failures and operational safety management as a result of their findings. It also included two instances of radiation leak, their cause, and noted no danger to the amount of radiation that leaked.

Actions currently in place –

- Minister's orders of July 16:
 - Minister's orders to TEPCO: Analyze cause and report the countermeasures on the inadequacy of facility's fire fighting system.
 - Analyze cause and report countermeasures for reporting delay of radioactive release.
 - Suspend plant operations until safety is confirmed.
- Minister's orders to all licensees on July 20
 - Reinforce fire fighting capabilities
 - Establish quick and accurate accident reporting system
 - Confirm seismic safety, prioritizing public safety

- Established an Advisory Committee (July 31)
- Established Fire Prevention and Protection Office at NISA (August 23)

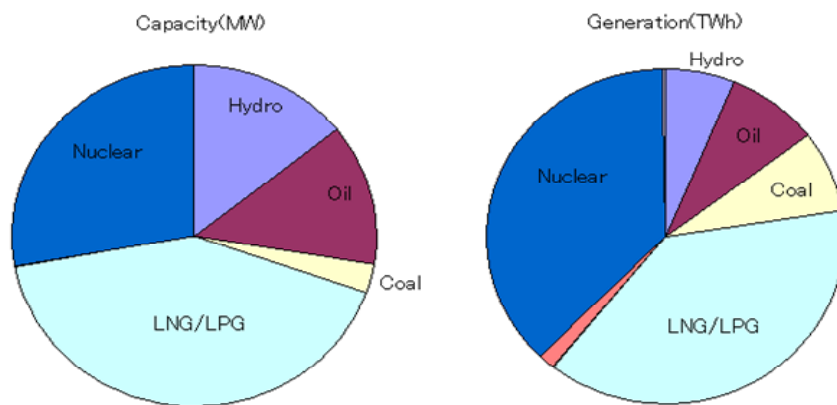
The way forward for NISA is to ensure that standards across licensed facilities in Japan are established and maintained. To this end, NISA’s newly formed advisory committee will review fire-fighting, reporting, and public relation plans and systems at all of its licensed facilities. It will evaluate seismic safety overall given the lessons learned from Chuetsu-oki earthquake data, and review procedures at other facilities. NISA also intends to hold a work-shop/seminar inviting international specialists with the intent of sharing lessons learned from the Kashiwazaki-Kariwa experience.

A second IAEA mission is planned to visit the nuclear power plant at Kashiwazaki-Kariwa, however, a date is not yet established.

Energy Supply: Composition, Capacities, and Earthquake’s Effect - Nuclear power provides 25 percent of the energy for Japan, and the Kashiwazaki-Kariwa nuclear power plant is--one of the largest power plants in the world—provides 10 percent of TEPCO total energy capacity. The effects of it not being able to produce energy as safety standards are verified can be significant. The chart below indicates the size and magnitude of the plant vis-à-vis other power stations, and shows the various sources of TEPCO’s energy by proportion.

Before the earthquake, estimated capacity to supply power for the Niigata area was 65GW, and planned demand at that time was 61 GW. In the aftermath of the earthquake capacity in July was down to 59 GW, and 58 in August; margins were extremely tight at a time when temperatures peaked in the region. Typical planning margins are at least three percent. Mitigating some of the demand was the Obon holiday when many families travel away from home. Nonetheless, to accommodate the reduction in energy production capacity various countermeasures were taken. These countermeasures included

TEPCO Energy Sources



Capacity of Nuclear Power Stations

Fukushima Dai-ichi	6 units	2,696 MW
Fukushima Dai-ni	4 units	4,400 MW
Kashiwazaki-Kariwa	7 units	8,212 MW

public outreach to constrain consumption were possible, augmentation of additional supply capacities (4.7 GW), contracted/coordinated cutoff of supply in emergency situations (1.28 GW), and emergency use of pump storage (0.9 GW).

Mr. Richard McPherson: Lessons Learned of Earthquakes and Nuclear Power Safety

Recording events such as the Niigata-ken Chuetsu oki Earthquake have formed a knowledge base contributing to nuclear power safety. The lessons learned from such events have strengthened our knowledge of what to do both before and when seismic activities occur to bolster safe operations. Collecting and sharing this knowledge makes nuclear power safer every year. One area making significant contributions to nuclear safety is the study of seismic activities, contributing improvements in plant designs.

Key elements of designing nuclear power systems cover a broad spectrum. Some of these are:

- Reserve capacities – management of energy utilities should include reserve capacities as a part of planned contingencies to preclude a shortfall of supply.
- Fire suppression capabilities – A nuclear power plant should have its own fire suppression capabilities that do not rely on local resources. A competent fire brigade should be able to suppress fires in a variety of contingencies and although this will increase costs, it is necessary element of the plant.
- Maintaining capabilities independent of local support – As noted above for fire suppression capabilities, a nuclear power plant design should include sufficient overall capabilities to address contingencies that do not rely on local support.
- Internal communications – Safe operation require sufficient internal communications not only for normal operations, but should also be capable in extraordinary situations.
- Public communications – Keeping the local community and overall public apprised of the functions, internal situation of a nuclear power plant is an essential element in contingency situations. Requirements for distributing information to the public should be a part of overall contingency plans
- Training – Nuclear power safety is a collection of lessons learned over decades. Incorporating lessons learned, and reinforcing actions to be taken throughout a spectrum of routine to urgent situations is a key element to nuclear safety.

The lessons learned in the world-wide commercial nuclear power industry for over 50 years have resulted in a safety record unmatched in human history, and should these lessons learned world-wide should be applied to training at all levels, both inside and beyond the company producing electrical power.

Session Number 2: Panel on Best Practices and Constructive Approaches for Planning and Executing Compliance Management

Presented by:

-Mr. Scott Smith; Economic Section, U.S. Embassy, Tokyo

-Mr. TAKAHASHI, Masakazu; Microsoft

-Mr. KITAGUCHI, Takaya; Executive Manager, Disaster Prevention, NTT Corp

This second session addressed the importance of government and private sector cooperation in preparation and response for critical infrastructure protection. Unlike the first session which focused on the aspect of nuclear power plants among the spectrum of critical infrastructure concerns, this session addresses a broader aspect of integrating capabilities, resources of government and industry. Presenters represented government and private sector views, and addressed the core theme of the conference reflecting the importance of integrating public and private capabilities and assets to effectively implement infrastructure protections.

Mr. Scott Smith: Comprehensive Approaches

Critical infrastructure protection is an event of scale that requires preparations for plans, response and recovery. The scope of critical infrastructure protection includes both government and industry participation in these areas, as facilities to be protected, authorities, and assets do not rest exclusively with government or industry. Both must therefore cooperate for infrastructure protection to be successful. Furthermore, both sides should resist compartmentalization, the notion that responsibilities reside with others, and incentives should be developed to take on appropriate risks. All involved should do all of these things in an effort to prepare against the unexpected. At the same time, both should realize that a feature of our globally integrated society is dependence on critical business systems which have become a part of life around the globe. CIP requires government coordination and planning, while simultaneously requiring cooperation of various industries.

In tackling the challenges of CIP, one may look at aspects of the issue from two perspectives. CIP naturally has a degree of specialization considering various systems involved; however, it requires a generalist approach to effectively plan and manage protections and responses necessary. Micro and macro perspectives lead to different conclusions which complicate the challenges of CIP.

Micro	Macro
Effects the individual, family, work, and business	Effects the functions of economy, well-being of the population, and government's ability to work and interact
Relieved when it happens somewhere else	Effects us all
Can be a sense of threat, as in an earthquake or act of terrorism	More appropriate to think of in term of risk, or choices in management of organizational structures, efficiency of cost, investments in protection

Globalization has several positive aspects; however, its effects also provide shocks which for which we must be prepared to address. These shocks may be the result of man-made efforts, or natural disaster; both of which involve preparing and responding to events of scale. Reflecting three themes of conservation (the three R's of "reduce, reuse, and recycle", perhaps CIP should consider a theme of "Robust, Resistant, and Resilient." Managers should consider robust aspects in their design of organizations and systems requirements that are strong, efficient and effective. They should be resistant to shock, and have built in resilience that can be responsive to change and able to recover from the unexpected. Our organizations—both governments and industries—should incorporate these factors to contribute to infrastructure protections. As governments proceed to deal with the challenges of infrastructure protections, they must realize that most of the infrastructure that must be protected are not government or public assets. A nuclear power plants is an example of this; it demonstrates that cooperation between private and public sectors is absolutely necessary to successfully accomplish infrastructure protections. Given this, we must challenge ourselves by asking how effective is cooperation? This in turn leads to an examination of areas such as:

- Levels of information sharing
- Drawing private sector views and concerns
- Level of integrating government policy objectives with planning, exercises, participation, and working together overall

While it is inevitable that we organize ourselves to respond to yesterday's problems, we should also recognize that events of scale are unpredictable. We should therefore consider contingencies beyond what we have already experienced, and the events that may occur unexpectedly. Some examples of this could be why SARS bypassed Japan, and despite this vulnerabilities in Japan; pandemic concerns given our means of mass transit and effects on critical sectors of utilities, health care, and financial transactions should a pandemic occur.

Mr. TAKAHASHI, Masakazu: Information Technology and Computer Security

The past 28 years witnessed development of information technologies and computing from stand-alone systems to the integrated network of computer systems operating today. Developing on a parallel track with IT systems were various threats, initially targeting operating systems. As networking became more sophisticated, threats to IT networks themselves.

Computing, networks, and threats have become fully integrated in these operations and with this vulnerabilities have expanded as a result. Threats can inflict severe damage within seconds. Two characteristics worth noting in terms of IT threats are *homogeneity* and *simultaneity* of threats, and *heterogeneity* and *asynchronies* of risks.

Homogeneous and simultaneous effects are pronounced when similar platforms face the same threats at the same time. Heterogeneous the asynchronous aspects of risk refer to the notion that individual platforms could have different risk levels depending upon unique countermeasures used against threats.

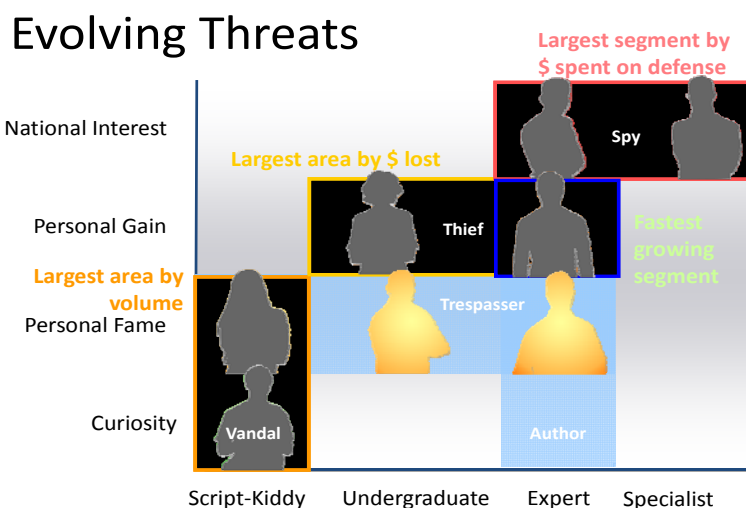
Networks, particularly the effects of the internet, have raised the efficiency of computers but have also raised vulnerabilities by providing an infrastructure for spreading threats. In 2001 Code Red, Nimda, and SQL Slammer viruses appeared, and they relied on networks to spread their effects around the world. In many cases the virus infected vulnerable computers within minutes. Firewalls were to protect networks; however security shortfalls—or holes—allowed viruses to spread rapidly. In the ROK the IT infrastructure broke-down as ATM machines could not operate, flight reservations could not be made, and the internet backbone itself failed. The volume and speed of traffic multiplied the effects of worms and viruses on networks. It became evident that cooperation between telecommunications and IT professionals was essential securing networks..

Microsoft responded with a philosophy called “Trustworthy Computing” in 2002. This approach to securing networks rested on four pillars: Security, Privacy, Reliability, and Business Practices. The basic approach to the security pillar was to emphasize investment in technology, development of prescriptive guidance, and forming partnerships within industry and government. Furthermore the approach sought to build security into systems by design; default, at appropriate settings; and in deployment of products and systems.

When securing systems in design Trustworthy Computing aims at ‘security development life-cycle’, which includes response to events as they occur. Security development life-cycle intends to provide security for the total life-cycle of the product. Security design does not stop at a product’s launch, rather it continues for the life-cycle of the product. As an example the initial six-months after Vista’s release, various security issues

developed for which countermeasures were developed.

Threats to IT and computing are changing in sophistication, their motivation, and severity. Early threats to computers required relatively unsophisticated skill levels to cause mischief motivated by curiosity or entertainment. The matrix below illustrates the evolving nature of threats, and shows that the fastest growing segment of threats to networks is from the highly skilled individual posing the most severe and costly types of threats.



Mr. KITAGUCHI, Takaya: Niigataken Chuetsu-Oki Earthquake: NTT Response and Lessons Learned

NTT learned many valuable lessons from a 2004 earthquake in Niigata-ken. One lesson is that there are three major areas requiring response on the part of telecommunication companies in this type of disaster. The three areas of damage key to telecommunications requiring response were facilities, power outage, and management of communications traffic in the aftermath of natural disasters.

Damage to Facilities – Damage to facilities include buildings themselves, the equipment within structures, and outdoor components. Architecture has significantly reduced the effects of earthquakes through design. There was no significant damage to buildings after the July earthquake, however one truck cable was severed. Fortunately multiple routes enabled traffic to flow without interruption.

Power – Approximately 37,000 households were without power after the earthquake. NTT gained lessons learned during the 2004 earthquake and reinforced its ability to respond to contingencies. Six telecommunication facilities experienced power outages, however all these locations were prepared with backup batteries; NTT was also prepared to further respond with generators mounted on trucks that were deployed to further support these installations. There were eight cases of remote terminals affected due to power outages. Most of these installations, however, were also equipped with backup batteries and also further augmented with mobile generators. Five of these remote terminals were augmented with mobile generators; however, trucks mounted with mobile generators were not able to reach three others due to vehicular traffic congestion. As a result 800 subscribers lost service, however this was restored the next day. As a result of the lessons learned from the 2004 earthquake, NTT was better prepared to respond to power outages by equipping itself with five times the mobile generators and trucks to deliver emergency power.

Telecommunication Transmission Surge – Emergency situations precipitate a surge of telecommunications traffic of which most transmissions are not high in priority. NTT experienced a large number of calls from outside the earthquake affected area; the Niigata-ken experienced 15 times the normal telecommunications traffic. Cell phone traffic—some of which was from within the effected area—was 40 times the average. When a surge in telecommunication traffic occurs many are not emergency calls; a high volume of traffic could cause the collapse of the system which would preclude critical transmissions in support of the relief effort. Responding to a surge in telecommunications traffic was therefore critical to ensuring that the system could continue to function, particularly to facilitate transmission of high priority connections. NTT managed telecommunication traffic by constraining non-emergency transmissions, and facilitating emergency calls. NTT constrained approximately 90 percent of incoming calls from outside the area affected by the earthquake, as well as outgoing cellular calls from within. Furthermore, traffic managers assigned priority to emergency numbers; the 110 and 119 emergency numbers in Japan, as 911 in the United States, were prioritized over routine calls. In addition to 110 and 119 calls, NTT also prioritized transmissions to and from designated emergency relief agencies.

Many of the lessons learned from 2004 eased telecommunication industry's response and mitigated collapse of the system. Still NTT recognizes that continued management of telecommunications during a disaster is challenged by the transformations within the industry, such as migration of telecommunication traffic to VOIP.

**Lunch Keynote: US-Japan Cooperation for Disaster Relief
Rear Admiral James Kelly; Commander, U.S. Naval Forces, Japan**

As a preface to his presentation on U.S. Navy nuclear power in Japan, RADM Kelly provided a briefing covering broad areas of the U.S.-Japan defense relationship, an update of security activities of the U.S. Navy and Japanese Maritime Self-Defense Force. Noting the

responsiveness and critical role that the JMSDF performs in the Indian Ocean, the Alliance's Navy-to-Navy relationship fulfills important maritime security missions extend beyond the region. Raising two recent cases to secure sea lanes of communications, RADM Kelly summarized actions taken by the USN to overcome piracy in the 7th Fleet area of responsibility. The two cases were of a Japanese-owned benzene transporter hijacked off the coast of Somalia, and a North Korean vessel similarly seized in the same area. The USN recovered both vessels, demonstrating that maritime forces securing sea lanes of communications, and transport vessels are very much pieces of critical infrastructure on a regional scale.

Yokosuka is the most important navy base in the world, not only because of its location, but because of the assets there: logistical capabilities, such as the six dry-docks—one of which is capable of supporting a carrier; its base force include nine AEGIS ships all capable of searching, detecting, and tracking incoming intercontinental missiles; five of these nine AEGIS ships (ultimately seven) are capable of launching SM-3 missile defense interceptors able to reach exo-atmospheric levels. Two key elements are the JMSDF presence with and the City of Yokosuka both of which the USN enjoys an extremely close and cooperative relationship.

The USS GEORGE WASHINGTON (CVN 73) succeeds a line of conventionally powered carriers that served in East Asia with a home is Yokosuka. Though the GEORGE WASHINGTON is only 10 percent larger than KITTY HAWK, its capability and capacities are significantly greater. The GEORGE WASHINGTON's power plant is obviously more capable and cleaner. U.S. Navy nuclear power is the safest in the world, and has never had negative incident raising risks in the air, water, or ground. It is a result of 60 years of experience to bolster safe practices. There have been over 1,200 visits by nuclear powered warship to Yokosuka, Sasebo, and White Beach Okinawa without incident. The nuclear powered carrier capability to conduct sustained operations is increased by over two-fold compared to the conventionally powered KITTY HAWK. Although GEORGE WASHINGTON and KITTY HAWK both have the same fuel capacities, no diesel fuel is required to power the ship, only aviation fuel to power aircraft. The USS ABRAHAM LINCOLN required no refueling during the two months of humanitarian relief operations in the aftermath of the 2005 tsunami.

USN participated in a natural disaster exercise Sep 07 in the metropolitan Tokyo area. Participating USN forces included the amphibious ship USS JUNO with two Landing Craft Air Cushioned (LCAC) vehicles which were used to evacuate citizens from the City. Naval forces proved to be a capable asset in this earthquake driven scenario which eliminated ground transportation with impassible roads. The USS GEORGE WASHINGTON will add to this capability, with greater responsiveness than the KITTY HAWK. The KITTY HAWK is able to reach a top speed of 33 knots with all eight boilers at capacity, but requiring nearly half a day to reach this speed; the GEORGE WASHINGTON will be able to reach 34 knots in 20 minutes.

3.16.14

While the USN and JMSDF enjoy an extremely close relationship rooted in military-to-military operational matters, RADM Kelly emphasized the importance of CNFJ's relationship

with City of Yokosuka in terms of critical infrastructure protection. Distinguishing the difference between nuclear weapons and Navy nuclear power, he acknowledged the strong anti-nuclear weapon sentiment in Japan while emphasizing the benefits and contributions of nuclear power to the naval force. Planning and conducting CNFJ-municipal response exercises are important. Through cooperative efforts, CNFJ was able to explain to the City of Yokosuka Mayor and other City leaders that exercising evacuation of the City in response to a radiological leak was unrealistic. Rather there were other realistic measures that required planning and response at a more local level. Furthermore, the Commander CNFJ, Mayor of Yokosuka, and Commander Naval Fleet Activities Yokosuka developed a unique memorandum of agreement to share assets in situations requiring response, concluding that for the U.S. Navy in Japan, trust is the most important element in the relationship to cooperation successfully between CNFJ and Japanese communities.

Session Number 3: Panel on National Cyber Attack/Cyber Crime and Countermeasures

Presented by:

-Mr. ISHIKAWA, Shoichiro; Director, Security Planning Division, Security Bureau, Japan National Police Agency

-Mr. Phil Sodoma; Director International Security Strategy, Microsoft

Mr. ISHIKAWA, Shoichiro: Cybercrime and Cyberterrorism Countermeasures; Security Measures for the G8 Hokkaido Toyako Summit

Cyber-crime is committed through the abuse of information technology in various ways. There are three broad categories of cyber-crime, all of which are rapidly increasing:

- Unauthorized Access to Computers which includes unauthorized use of passwords and identification.
- Unauthorized use and manipulation of electromagnetic data
- Unauthorized use of networks, such as acts in support of fraud, child pornography, and use of networks related to copyright and trademark violations

Japan's National Policy Agency (NPA) is organized to address cyber-crime at the national and prefectural levels. The NPA is responsible for overall guidance and coordination, however it is integrated with two departments of prefectural police organizations: investigation departments and information-communication department. The investigation department collects information and evidence, while information-communication departments provide technical skills for electromagnetic forensics.

Cyber-terrorism has no universally accepted definition; however the NPA defines cyber-terrorism as cyber attacks on mission critical systems or critical infrastructure, or failure of critical infrastructure due to cyber attacks. Cyber-terrorism

is viewed as a subset of cyber-crime. Critical infrastructures are those areas which provide basic necessities to daily life, and social activities, the scope of which is outlined in the ten areas listed below:

Info-communications	Gas utilities
Financial Sector	Government/Administration
Airlines	Medical Sector
Railway	Logistical sector
Power utilities	Water supply

While many benefits of IT development, the systems have become complicated and identifying the cause and source of cyber-terrorism has grown increasingly difficult. Japan has yet to experience a catastrophic case of cyber-terrorism, however there have been several cases of cyber-crime. In 2004 attacks on government IT systems spiked after the Prime Minister's visit to Yasukuni, and in April 2005 as anti-Japan riots occurred in China. Japan experienced two other serious cases of cyber-attack in September and December 2006 on the Bank of Japan's IT systems.

Critical to countering cyber-terrorism is cooperation between public and private entities at various levels. Unlike cases of cyber-crime, prefectural security departments and the NPA's Security Bureau become engaged in cases of cyber-terrorism. Also in cases of cyber-terrorism a cyber force is formed at the national and prefectural levels to bolster technical capabilities and to enhance information exchange.

Public-Private cooperation is a key element of countering threats. The NPA facilitate cooperation placing emphasis on three areas. First, the various cyber forces make regular visits to critical infrastructure proprietors; second, the police provide updated information; and third, the police hold counter-terrorism conferences with key proprietors at the prefectural level focusing on information exchange. Thus far, six prefectural conferences have been formed.

Another key aspect in countermeasures is conduct of joint exercises between police and critical infrastructure proprietor. During these exercises, participants focus on advancing early detection, rapid reporting to police, how to minimize damage.

To bolster the technical aspect of fighting cyber-terrorism, the NPA maintains a Cyber Force Center on a 24/7 basis to conduct real-time detection of network systems, and botnet observation. This national center is supported by eight regional centers to provide emergency response, and early detection of cyber-attacks.

G-8 Summit and Ministerials: Countermeasures against Cyberterrorism

Japan will host several ministerial meetings, and the summit for the next G8 summit meeting to be held in Hokkaido 7-9 July. Ministerial meetings will be held from April through June at various sites throughout Japan. Japan's National Police Agency recognizes that the

threat in broad terms comes from international terrorist organizations, and anti-globalization activists. Previous meetings at Genoa (2001), Evian (2003), Gleneagles (2005), Heiligendamm (2007) provide a preview of the type and magnitude of activities realized by the threat. As a result, the NPA is taking an approach against cyber-terrorism called “Two Prong-Plus Alpha”. It indicates the requirement to focus on two locations: the meeting venue and major metropolitan areas. However, the “Plus Alpha” indicates the importance of also focusing adequate attention to cyber-space.

The approach requires identification of infrastructure sectors at the venue which could become potential targets for cyber attacks. This includes the ten sectors for cyber-terrorism protection identified above, the press center, and the physical venue site of the summit. Major metropolitan areas will require coordination with administrators of critical infrastructures in identifying system vulnerabilities, and diagnosis for improving information security. As noted above, joint exercise will be an important aspect of preparation. Joint exercises with the town of Toyoko and critical infrastructure proprietors such as NTT DoCoMo have already been conducted. Because cyber-threats are not limited to geographic locations, several other joint exercises are planned for locations throughout Japan.

Mr. Phil Sodoma: Preparation for National Level Cyber-crime/Cyber-Terrorism

As noted earlier, the cyber-crime threat environment is undergoing change. The earlier threat environment was comprised of less organized efforts seeking fame and notoriety. The current threat environment is being formed by entities with greater skills and organization. They are motivated by financial gain, operating at a lower profile than earlier models. Although previous threats functioned within a broader scope of targets, the current threat focuses on specific companies and brands. An example of the new threat is “Rockfish” which operates from within Russia. Rockfish is a small group of well organized individuals operating in cybercrime. It is comprised of compartmented entities each with specific responsibilities, such as development of codes for malicious attacks, operations, and finance. They maintain a low profile by targeting relatively small amounts of money, and by shifting the targeted industry; by doing this, they avoid the attention of law enforcement agencies that would otherwise be motivated to pursue the threat. However this small group will gather over \$100 million per year through these practices, while also selling their technique to others with malicious intent. Botnets and botnet storms--another new feature of the threat environment—are proliferating. They operate with as many as a million to tens of millions of computers transmitting spam.

Cyber threats now target SCADA systems (Supervisory, Control and Data Acquisition Systems) operate across the CIP spectrum, including power generation, other utilities, and manufacturing systems. These systems are intended to operate for long periods of time (20-30 years), and therefore typically do not have security systems that are frequently updated. Because they are an aspect of controlling various aspects of key infrastructure, they form a new area of vulnerability that should be integrated into CIP security systems.

Essential to comprehensive CIP preparation and response are various areas due to the complexity of critical infrastructure and security. These include:

- Policy: necessary to establish strategic direction and guidance
- Law enforcement: Strong criminal and civil actions by government and industry to punish and deter criminal activity
- Technical: research and development to increase infrastructure resiliency, and to apply existing technologies to security systems; to create solutions and controls
- Organizational: Bring alignment and connections for effective communications bringing rapid information transfer against developing threats.
- Education: promote user awareness in all audiences
- Important aspect of responses
 - Global solutions: requiring information sharing and policy framework
 - User-focused: technology and education to address weak links
 - Based on strong public-private partnerships

As mentioned by several presenters previously in this forum, close government and industry integration and cooperation is essential. Government has various authorities and can coordinate IT securities, however much of the infrastructure that is to be protected belongs to private entities. In the U.S. there are several entities that take this approach. Government itself has various agencies and offices which require coordination for CIP; in the U.S. CIP is comprised of 17 critical sectors, one of which is IT. Each sector builds specific plan and sets a strategic direction among various aspects of government, enterprises, and industry participants for CIP in the IT sector. The Information Technology Sector Coordinating Council (IT-SCC) is the body which does this for the IT sector. The Information Technology Information Sharing and Analysis Center (IT-ISAC) is an organization whose role is to communicate current vulnerabilities, threats, and sharing information within the U.S. Another key entity is the National Security Telecommunications Advisory Committee (NSTAC), in which Microsoft executives play an active role. This body works on next generation networks and developing increased resiliency for the IT sector.

The IT Sector Specific Plan generated and released by the Sector Coordinating Council has been issued and is publicly available³. There are three key goals in the Plan.

Prevention and protection through risk management. The IT sector took a somewhat different approach than other sectors. Because IT assets operate virtually across various physical assets, the traditional security approach that would normally begin with identifying physical assets to protect is not appropriate. Rather, the IT sector decided to examine the critical *functions* that it has to produce, and upon identifying the *functions*, the IT

³Department of Homeland Security, "Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan", May 2007; http://www.nascio.org/committees/security/IT_SSP_in_InDesign3.pdf

sector would proceed with risk management by identifying vulnerabilities, threats, and actions to be taken to mitigate risk.

Situational Awareness. Improve situational awareness by ensuring good communications and technologies for sharing information during normal operations, potential or realized threats and disruptions, intentional or unintentional incidents, crippling attacks (cyber or physical) against IT Sector infrastructure, technological emergencies and/or failures or disasters declared by the President.

Response Recovery, Reconstitution. Enhance the capabilities of public and private sector security partners to respond to and recover from realized threats and disruptions, intentional or unintentional incidents, crippling attacks (cyber or physical) against IT Sector infrastructure, technological emergencies and/or failures, or disasters declared by the President, and develop mechanisms for reconstitution.

Mr. Richard McPherson: Nuclear Safety and U.S. Navy Nuclear Power

Nuclear power generation has operated for over six decades with an extraordinary safety record. The U.S. Navy excels at nuclear power safety which it achieves through processes of selection, education, testing, surveillance, and the accumulation and implementation of lessons learned. Demonstrating the safety record of nuclear power, Mr. McPherson juxtaposed the effects of smoking a pack of cigarettes a day for a year, and the safety level of radiation exposure for those working on nuclear power plants. The effects of smoking a-pack-a-day for a year results in an accumulated exposure level of 5 REM⁴ in the body. Safety standards of the U.S. Navy restrict its nuclear power plant operators from continuing to work on nuclear power plants should they reach one-fourth that level. Adding to this, he noted that after 45 years of working with Navy and commercial nuclear power plants—of which his exposure and activities have been constantly monitored and recorded—his accumulated lifetime dose is 8 REM.

Opposition to Nuclear Energy

"Opposition to nuclear energy is based on irrational fear fed by Hollywood-style fiction, the Green lobbies, and the media. ... Even if they were right about its dangers - and they are not - its worldwide use as our main source of energy would pose an insignificant threat compared with the dangers of intolerable and lethal heat waves and sea levels rising to drown every coastal city of the world. We have no time to experiment with visionary energy sources; civilization is in imminent danger and has to use nuclear, the one safe, available energy source, now, or suffer the pain soon to be inflicted by our outraged planet." *London Independent – May, 2004*

⁴REM (roentgen equivalent man): A measure of dose deposited in body tissue, averaged over the body. One REM is equivalent to 0.01 sievert.

Mr. McPherson noted that many do not realize the effort and achievement of nuclear power operations. He shared what he viewed as the most succinct expression of its safety, stripping away fictional hyperbole.

Nuclear power is safe, and becomes safer every year. There are 436 nuclear power reactors in 31 countries, France has 59 commercial plants, and Japan 55. There are 103 commercial reactors in the U.S. and 109 U.S. Navy reactors. Overall, nuclear power has 10,000 years of operations.

Navy nuclear power has been at the forefront of nuclear engineering, from its start in 1948. Of the 10,000 years of total nuclear power operations noted above, the U.S. Navy has 5,800 reactor years of safe operations, over half of the world's total. Nuclear power has safely steamed over 135 million miles and is welcomed at 150 ports around the globe in 50 countries. These are the results of a nuclear power program that have emphasized processes of selection, education, testing, surveillance, and implementation of lessons learned. The U.S. Navy applies a rigorous selection processes in people, materials, design, construction, operations, and maintenance. Its education process includes every aspect of its nuclear program, is frequent, and never-ending. Surveillance and testing is a key element of the Navy's program in that it is an inherent part of the entire program. Maintenance, overhaul and testing, for example, are not based simply on a periodic schedule, but are integrated into constant surveillance of the system. Every aspect is meticulously recorded. Mr. McPherson explained parts and components as an example: For a pipe replaced on a nuclear system, the Navy will have recorded the location from which the material was mined; means, dates and individuals related to its transportation through the process of replacement, to include the individual who replaced it and that individual's record of certification.

Navy nuclear power development has created materials which can withstand higher temperatures, pressures, levels and duration of radiation which all raise safety levels. Mr. McPherson noted that materials are now available with higher tolerances that never before existed, raising the example of a pipe rated with maximum pressure specifications of 750 lbs, being replaced by materials with a bursting standard of 92,000 lbs. Another example of Navy contributions to advanced safety are magnetic bearings which preclude metal-to-metal contact and thus eliminating metal fatigue and wear.

The Navy is also improving efficiency. Mr. McPherson noted that the latest submarines are now powered by nuclear reactors that require no refuel for 33 years; the next generation aircraft carrier require no refueling, ever.

The future of nuclear power will depend on several areas. It will continue to depend on its record of safety, and all of the aspects to contribute raising safety measures. It will also depend on arrangements for the storage of spent nuclear fuel. Other factors that will be important to continued efficient use of nuclear power in the future will be educating the public on the facts of nuclear power, developing new designs, international cooperation for continued

supply of fuel and associated logistical requirements for fuel, and private industry and government cooperation for these systems.

**Keynote Speaker – MR. HASHIMOTO, Shin; Executive Vice President NTT Corporation; Member of the Board, and Director of Next Generation Office
NTT's Vision for Communication Infrastructure Protection**

Protection of the telecommunications sector is becoming more challenging and complex. It is critical to governments industry, and individual households on a daily basis, but its importance skyrockets during crises. NTT was formally nationally owned; however is now a private entity. Its role as a critical infrastructure entity has been in place for several years, and it has gained many lessons learned in building its vision for communication infrastructure protection.

Mr. Hashimoto remarked that he was in the U.S. during the attacks on September 11th and was able to observe responses by various entities, noting that their motivation, urgency, and bravery were remarkable. Actions in the U.S. validated many aspects of NTT's vision for protecting the communications infrastructure. Japan has also had several crisis situations testing communications infrastructure from which NTT gained valuable lessons. One validated point is that information infrastructure, computer data systems, and the internet combine to support a sophisticated system of transmitting information; however it also means that all of these sectors rely heavily on each other. They combine to result in highly efficient transmission of information; however they also combine the effect of vulnerabilities on an overall communications system. Sophisticated data requires a critical infrastructure of underground cables to support transmission. Command and control during normal operations is important, however, during a crisis control centers are absolutely critical. The internet has bolstered efficiency, accuracy, and availability throughout in communication field. Likewise, this technological breakthrough subjects telecommunications to internet vulnerabilities and challenges to crisis response measures.

As a telecommunications leader, NTT realizes that it has a responsibility to be prepared for contingencies, and to respond at times of natural disaster and other types of emergencies. Furthermore, industry-and-government cooperation in planning and responding will be requirement to those responsibilities. Earthquakes, lightning, and typhoons make Japan a natural disaster prone country, and adding to this the possibility of criminal or terrorist induced damage to the communications infrastructure, NTT has a responsibility to maintain communications during normal and emergency situations. There are several NTT lessons learned that formed its vision for protecting communications:

The 1968 Hokkaido earthquake brought great devastation, and cable and wireless transmission lines were severed. As a result, all of Hokkaido was isolated for 2 hours; the

Prime Minister and rest of the nation had no idea what was occurring on the northern island. NTT then was a national entity and responsible for maintaining its operations. Its key lesson from this was the responsibility to think through and be prepared to respond to various contingencies. Another lesson was to be prepared for a surge of communications traffic at a time of crisis.

The 1982 flood in Nagasaki caused service disruption. Facilities were not built to withstand many of the pressures that extreme weather conditions imposed on NTT's facilities. The lesson NTT has learned is to fireproof facilities, and build embankments surrounding key structures.

In 1984 NTT operators working on underground cables caused a fire that ultimately destroyed a telecommunications office. It was at a time when NTT was undergoing its privatization transition and many argued that the introduction of market competition would result greater vulnerabilities to the communications system. It was a call for companies that serve the public to act responsibly. Mr. Hashimoto stated that for him, it was a reminder for utility companies to maintain their motivation and diligence in responding to disaster situations. During that incident NTT's leadership was not able to obtain key information of the problem and likewise subordinate offices were not able to communicate information to executives. It was an especially difficult time and a tough lesson learned.

The 1995 Hanshin Earthquake left 5,500 killed and over 200,000 houses destroyed. The devastation as it relates to the communications world, dropped service to 300,000 subscribers for more than a week. At the same time, the surge of telecommunications traffic rose to 50 times normal levels. By 2003 cellular use had grown, and the earthquake that year near Sendai, brought a new dimension to sustaining telecommunications with this wireless medium. NTT DoCoMo cell phone transmissions rose 20 times normal traffic.

To secure communications infrastructure NTT developed backup capabilities to critical points in their system, made facilities more resilient to disasters, and conducted 24/7 monitoring of the overall system. Response has been improved with portable satellite communications components, mobile base stations, and switching systems. These can be deployed via helicopter to re-establish systems. NTT found that it was not enough to simply rely on batteries for backup power, but that key installations had to have their own battery supplies on hand to respond quickly. NTT also maintains a 24/7 monitoring and control system to identify and communicate quickly the location and magnitude of system failures.

To address the problem of managing the surge of telecommunications traffic, NTT prioritizes calls. Lines dedicated to emergencies response organizations such as the police, government offices and other responders have priority. Simultaneously, announcements are sent notifying users that a constrained system is in place. At the same time it is clearly understood that many of the non-emergency calls are important transmissions notifying friends and relatives of their conditions and assurances of safety; denying this exchange of information

would be problematic. For this, NTT establishes a “Disaster Emergency Message Dial” service. The message service is operated within a town network and messages can be left on the service notifying friends and relatives that the individual/family is safe, and location to which they moved as a result of the disaster. This system is not limited to voice, but also has internet possibilities. A “Disaster Message Board” Service was formed for use through PC or cell phones to place similar information on internet based message boards.

Mr. Hashimoto noted that a major challenge to telecommunication carriers are the effects from integrated internet protocol-based networks. Carriers will have to be fast in taking on this challenge. This integration is occurring rapidly, such that by 2010 the industry estimates that 20 million subscribers will be on broadband network-based systems. This transformation has clear advantages for the telecommunications world. However, by integrating the benefits of the internet with traditional telecommunications systems, it introduced to the telecom world the vulnerabilities of the internet such as eavesdropping, and identification vulnerabilities. Furthermore, cyber terrorism could be used to target companies, governments, and other institutions. The telecommunications industry must therefore continue to improve its security measures for the traditional areas of its industry, but must also incorporate security measures which multiply vulnerabilities as the industry transforms.

Telecommunications is increasingly integrating its operations with other sectors. Security measures will therefore require the industry to cooperate with other industries and entities to counter growing vulnerabilities that emerge from this integration. To effectively secure this sector the telecommunications industry will be required work together with entities that may simultaneously be competitors. To ensure that this sector responds effectively and quickly, operators at every level must be properly trained, and the flow of reporting information will not be top down, but increasingly all will be involved. Motivation and initiative throughout the sector will be a key factor in making these protections successful.

Major General James Flock; Deputy Commander, U.S. Forces, Japan. Evening Speaker: Disaster Relief Operations in Japan and USFJ

MajGen Flock addressed disaster relief and U.S. procedures required leading to political decisions for the military to support. He described the interagency process among the Departments of Defense and State, and the National Security Council; noting that the Department of State has much of the lead in interagency coordination as it relates to a U.S. foreign policy decision. Other U.S. government entities that are involved in the interagency process could include FEMA, USAID, and others depending upon the requirements for relief and the effected area.

MajGen Flock noted that USFJ had made significant contributions to disaster relief in Japan. Several elements of USFJ had deployed to the Hanshin area in response to the 1995 earthquake centered on Kobe. More recently, USFJ responded with a disaster relief mission in

Niigata-ken when USFJ deployed equipment to support the overall relief effort.

Session Number 4: “Is Minneapolis the Tip of an Iceberg? Concern for Physical Aspects of Aging Structures”

Presented by:

-Dr. Michael Leineweber; Durant Media Five

-Mr. NISHIKAWA, Kazuhiro; Executive Director for Research Affairs; Ministry of Land, Infrastructure and Transportation

-Mr. TAKAGI, Sentaro; Tokyo Metropolitan Government

Dr. Michael James Leineweber: “Is Minneapolis the Tip of an Iceberg? Concern for Physical Aspects of Aging Architecture”

Dr. Leineweber noted that a society’s quality of life is typically reflected in its civic architecture and infrastructure and since the 1964 Olympics; Japan has impressed the world in this regard. The Shinkansen, highway system, and buildings are a reflection of Japan’s re-emergence after the war. Many of these structures in both our countries’ are aging and deteriorating. On August 1, 2007 the Mississippi River Bridge in downtown Minneapolis, Minnesota collapsed during the 6PM evening rush hour reminding us of this and the importance of infrastructure protections.

Response - The bridge was designed with a support structure under its roadway which was a typical design of its day. Because the support structure was below the roadway, there was no overhead steel. There were 13 fatalities and 100 injured, relatively small numbers given the magnitude of destruction. The response was complicated by the variety of authorities involved. Minneapolis’ Director of Emergency Preparedness summarized the complexity of the scene: this collapse was of a State bridge, over a county river, between two banks of a city. However, these complications were overcome before the disaster occurred because of planning, training, and exercises. All responders knew the organization of assets and operations throughout the response.

City, county, and state officials had trained for disasters with support from FEMA since attacks on September 11, 2001. Initial response came from civilian volunteers, followed by local fire, police, rescue and medical. Emergency services arrived within 6 minutes and helped people trapped in their vehicles; 93 victims were rescued from the collapsed bridge the first day. The City of Minneapolis Collapse Structure Rescue and Dive Team, and Emergency Operations Center were established within 15 minutes of the bridge’s collapse, and all could communicate with each other. Minneapolis Fire Department established a National Incident Management System Command Center in parking lot of on the west bank of the river; Minneapolis police secured the area, Minneapolis Fire Department managed ground operations; and Hennepin County Sheriffs Dept managed water operations. Because water operations were

hampered by debris in the water, the Army Corps of Engineers lower the water level about 2 feet to allow greater access.

In the aftermath of September 11 and the formation of the Department of Homeland

**Mississippi River Bridge
Minneapolis, Minnesota**

Opened in November 1967
 Dimensions:
 Length: 1907 ft (structure length; 458 ft (length of max. span)
 Width: 8 traffic lanes, 108 ft
 Height: 64 ft above water
 Location: I-35 West at Mississippi River mile marker 853.20 and 1 mile northeast of junction TH94
 Type structure: Steel Arch Deck Truss
 This bridge is unique because it was constructed with a single 458 ft steel arch to avoid putting piers in the water which would impede river navigation.
 Daily Traffic: 141,000 vehicles per day as of 2004 count.

Security, governments trained and invested in disaster response. The State of Minnesota and US Department of Homeland Security invested in mobile radios affording Federal, State, and three of the responding counties immediate communications throughout the response.

Inspections – The State of Minnesota had identified the Mississippi River Bridge as “structurally deficient” in 1990 and programmed for its replacement in 2020. Since 1993 Minnesota Department of Transportation inspected the bridge annually, with the exception of 2007 when the planned inspection was postponed due to ongoing construction.

In 1990 the Federal Government rated the bridge “structurally deficient” citing significant corrosion. “Structurally deficient” is a classification that does not mean in and of itself that a structure is not safe; there are over 75,000 other structures with this classification in 2007.

In 2001 the University of Minnesota’s Civil Engineering Department conducted an evaluation for the State Department of Transportation. This report noted that although there was fatigue on the steel trusses, there was no cracking and no need to replace the bridge. It noted a lack of redundancy in the main truss system, indicating a greater risk of collapse in event of a single structure failure. The report concluded that continued monitoring of the structure was warranted. In 2005 the U.S. Department of Transportation rated the bridge “structurally deficient”. In 2007 a consulting company recommended that gusset areas be reinforced with metal plates. After the collapse on August 1st, Governor Pawlenty announced

that his understanding of the reports was that the bridge would be safe for operations until 2020 or beyond. The U.S. Congress passed legislation appropriating funds in support of replacing the Mississippi River Bridge, and \$1 billion to support states fix deteriorating bridges.

Since the collapse, the National Transportation Safety Board began its investigation and its findings are expected to take about 18 months. President Bush designated U.S. Secretary of Transportation Mary Peters to lead the reconstruction effort. Foundation for the new bridge is expected to begin soon, and it is planned for completion in December 2008, costing \$234 million dollars.

The lessons learned thus far from this disaster are boiled down to five points. Though there were many technical inspections of the bridge, there was no political response to the reports. Next the first responders acted swiftly and this saved lives. Third the governments rescue work was planned, practiced, and coordinated. Fourth, the investigation can take a long time, and there will be many legal complications. Fifth, political decisions are required to maintain and rebuild infrastructure.

Mr. NISHIKAWA, Kazuhiro: The Fear of Aged and Damaged Critical Infrastructure

The collapse of the Mississippi River Bridge in Minneapolis was a great surprise to city planners and structural specialists in Japan. It occurred as the Ministry found severe cases of structural deficiencies caused by corrosion in Japan. One was on June 20 this year, when Land Ministry inspectors found structural damage to trusses on the National Highway 23 Kiso River Bridge. The same type of deficiency had been discovered nine years earlier in 1999 where corrosion caused deterioration of “H” beams, however, follow-up lessons learned did not identify the Kiso River Bridge until severe damage was evident. As a result, the central government directed a nationwide inspection program of all bridges, during which several deficiencies were discovered.

A month after the Minneapolis disaster, the Honjo Bridge on Highway 7 was found to have severe corrosion. The road was closed and administrators scheduled work to rectify deficiencies. As a large crane crossed the bridge, inspectors saw one of the corroded beams spread open before their eyes. Planners believed that paint protected the bridge’s steel components from corrosion, but discovered instead that severe corrosion deteriorated the structure over time. Inspectors found that the paint itself—used to protect the steel—deteriorated due to alkali in the concrete. These two incidents caused infrastructure managers to take additional action. A National program was initiated to develop incentives for local governments to take greater initiative to maintain bridges.

Officials responsible for maintaining road and bridges were faced with a question: Which posed the greater danger, earthquakes or aging structures? The catastrophic and sudden effects of earthquakes more easily seizes public attention. Japan had been working to focus on the maintenance of aging infrastructure in the early 90’s. However, the Great Hanshin

Earthquake in Kobe⁵ derailed the effort and shifted attention back to earthquake prevention and response. Japan's infrastructure is aging, and this could be a more serious problem since deterioration and the dangers they present could occur anywhere, anytime. The events in Minneapolis and these bridge deterioration discoveries are bringing a focus back to the importance of inspections and maintenance.

We are finding that there are hidden dangers of deterioration from salt. Most of Japan's highways and roads were built in the 60's, and run along the coast exposing roads and bridges to saltwater. Like alcohol to the human liver, Japan's civil engineers are finding that the damage caused by salt to bridges is not visible by observing only the exterior. As with liver damage, engineers must inspect for corrosion in places covered by concrete where the corrosive effects of salt is taking place.

Broad coordination is necessary for road and bridge maintenance. They require political leaders to make them a priority and provide an adequate budget for the cost of maintenance. Also lesson is that procrastination is dangerous in this work; time works against effective maintenance, and presents risks to safety.

Mr. TAKAGI, Sentaro: Changeover to a Preventive Maintenance Type Control in the Tokyo Metropolitan Government

Mr. Takagi described in detail aspects of the Mississippi River Bridge collapse in Minnesota as a technical expert. He addressed factors such as corrosion in various portions of the bridge, vibration, and other aspects that contribute to structural fatigue. His estimate concludes that major deterioration did not exist in the bridge's truss core, but that in truss panel points had fatigue cracks. His analysis leads him to believe that there were probably danger signs and that it is most likely that the effects of this deterioration could have been avoided through preventative maintenance.

Japan's bridges are getting older, raising the imperative of managing maintenance and the condition of these structures. In Tokyo, 49 percent of its bridges are over 40 years-old and bridges in the U.S. have similar percentages. In 10 years, 75 percent of Tokyo's bridges will be over 40 years-old. This raises the specter of funds for operations and maintenance. In Japan there are no subsidies for tests, inspections, or investigations on bridges. Local authorities bear nearly half the cost of inspecting and maintaining these structures. In the U.S. the Federal Government supports 80 percent of these costs, even if the roads and bridges are managed by a state government.

In Tokyo, city planners are trying to optimize infrastructure by building efficient maintenance into life-cycle programs. Factors in building an asset management system for its infrastructure will include estimating deterioration of structures, life-cycle costs, social benefits of the structure, construction to add longevity of structures. All of this will be supported by an

⁵Great Hanshin Earthquake occurred on January 17, 1995.

integrated database system to maintain key elements of information. By end of year, Tokyo will complete development of a mid and long-term plan for how to receive the best return on its assets. Political priority for maintenance is typically an area that does not receive much attention, however appropriating funds for maintenance and operations are necessary. Minnesota's bridge collapse has raised the attention level of infrastructure investment in Japan which is increasingly a critical matter as this infrastructure sector ages.

Keynote Speaker: Governor ISHIHARA, Shintaro

Governor Ishihara reflected on his impressions of September 11, 2001. Having been in the U.S. on that day, he had already met with several security policymakers such as Deputy Secretary of Defense Wolfowitz, National Security Advisor to the President Rice, and others and explained how he was impressed with the U.S. Government and its swift actions in the wake of attacks that day. The Governor advised Prime Minister Koizumi to take similar actions, but the Governor said the Prime Minister resisted, leaving it up to him to take some initiative. Governor Ishihara formed with the municipal heads of Kanagawa, and Saitama a FEMA-like organization that would coordinate information and actions among themselves, and with this body also coordinate with the central Government of Japan. They had no emergency means of communicating, such as a hotline, and noted that generally they were not well prepared to respond to this kind of crisis. Reflecting on this and other experiences that placed him in the position of political leadership, he explained that the unpredictable nature of many crises makes preparations difficult for political leaders.

Governor Ishihara explained that political decisions have often had negative effects on natural and manmade disasters. He raised his view of how the quagmire of the Middle East can be traced back to unrealistic promises made by the British to Palestinians. These were promises that the British could not keep, leading not to double standards, but triple standards in the region. He then posited that U.S. tensions of the Cold War led the U.S. to take sides with Taliban leaders when the Soviet Union invaded Afghanistan leading to the current state of instability in that country. Next, Governor Ishihara stated that Fiji is a case where Australia made worse a situation with good intentions. At Fiji, rising sea-levels are shrinking Fiji's land mass. In a response to help, Australia sent assistance that included food not healthy to Fijians. Finally, the Governor mentioned global warming as another example of how political decisions over a long time have created a broad negative situation.

Governor Ishihara described the challenges of emergency planning from the perspective of political leadership. In this regard, he mentioned that political leaders must also deal with the public's will to resist change, and that the size and complexity of large urban areas magnifies this issue for management in the metropolitan area. Governor Ishihara conveyed this through his impressions left by the Kobe earthquake over 10 years ago. He said that there are still several areas that have not fully recovered, and much of this is a result of people not wanting to move from areas that they have long identified as their home. Tokyo Metropolitan Government once had an office called Urban Planning Section, but has since renamed it the

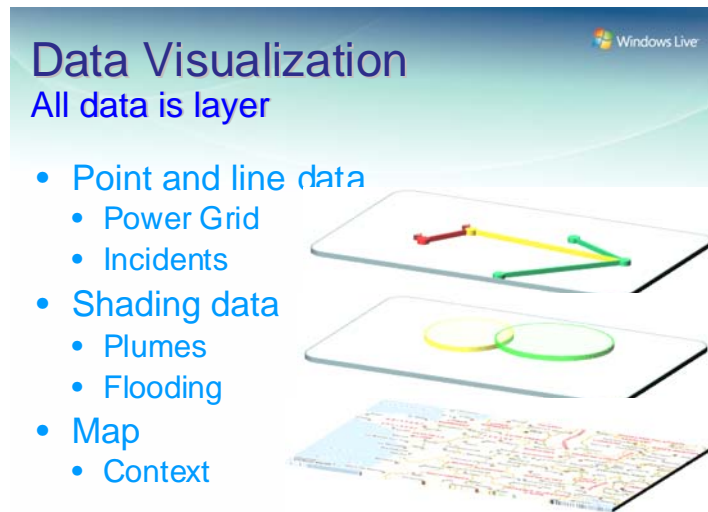
Urban Improvement Section because urban planning has been too difficult. Changing the urban landscape and developing better conditions for emergency response is very difficult. Roads are not sufficiently wide in Tokyo, and as a result first responders cannot move directly to a critical site. He added that changing these conditions requires a desire that the public must accept. Seeking public understanding for various kinds of change is an extremely important aspect to implementing many of the changes that improve disaster response in Tokyo and other urban areas.

In conclusion, Governor Ishihara pleaded with Americans to allow for the commercial use of aircraft at Yokota Airbase. He noted that Haneda and Yokota Airports are extremely busy and that 40 countries have requested additional routes into Japan. While expansion is being considered by these two airports, he argued that the longest runway in the area is at Yokota, and granting use of commercial aircraft at this U.S. military facility would afford the Tokyo metropolitan area better conditions for disaster response.

Roger Mall; Microsoft Corporation, Virtual Earth Business Development Manager
Imagery and Critical Infrastructure Protection: How Governments and Companies Are Using Imagery to Manage Risks, Enhance Operations, and Respond to Emergencies

Computer mapping and the use of imagery is not a new effort. Maps and imagery products appeared on computer screens first in 1969; online mapping applications appeared in the early 1990's in the form of MapQuest on the internet. Since that earlier time, digital imagery has become widespread and broadly available. Data visualization combines these three technologies providing managers with a display to quickly grasp key developments, trends, and points of concern for which they are responsible. Maps married with applications that can be easily brought to business problems to develop solutions.

Data visualization combines various data by layering them on one image. The first layer provides the map or image base. The second layer adds business data, such as the critical infrastructure base of information. The third or successive layers add external data relative in position to the map and business data.



Several examples were raised to demonstrate data visualization for managers in various types of fields. All were demonstrated with some base data that produced a map or image where additional data could be superimposed which displayed various data in relationship to locations, either on the map or image. Many of these examples were drawn from the internet as recent as the earlier the same day. These examples included:

- Nebraska Public Power: An image from the morning of this presentation. It visualized locations on a graphic map of power outages. By identifying the outages graphically on a map, one could analyze the source of the power outage.
- Disease Outbreak of Avian Flu. On map of the Western Hemisphere, locations of Avian flu, with the migration patterns of birds supported analysis of subsequent areas of potential outbreak.
- Fire Risk Management: On a base layer of a map of Tokyo, a second layer data displayed various types of structures by area to determine levels of fire risk. Responding to the spread of fire requires speedy data layering to enable fire fighters to make quick, appropriate decisions. Matching two layers in this case could be done in 15 minutes or less.
- Traffic Management. The image of a traffic intersection as a base layer is used to superimpose traffic accident data, which enabled planners to visualize and analyze why accidents occur and how to make changes to reduce traffic incidents.

Although the separate forms of data and using each type individually is not an old technology, merging various kinds of data on maps and images to visualize data is a technology which transforms management. After this technology is used initially, managers—rather than the technology developer—become the source of new ideas for combining various technologies to address a variety of issues. The technology of data visualization simplifies the integration of

various data, and the integration itself can be done quickly.

Session Number 5: Panel on CIP Implementation, Accomplishments and Goals in Japan

Presented by:

Mr. YAMAGUCHI, Suguru; Government of Japan, National Information Security Center, Cabinet Secretariat, Advisor on Information Security

Mr. ARIMURA, Koichi; Telecom Information Sharing and Analysis Center (Telecom-ISAC Japan), Director Planning and Coordination Division

Mr. YOSHIDA, Teruyoshi; Center for Financial Industry Information Systems, Security and Audit Research Department

Ms. ITO, Yurie; JPCERT/CC, Director for Technical Operations

Mr. YAMAGUCHI, Suguru: Work of the National Information Security Center

The National Information Security Center (NISC) is the national level organization to coordinate and organize critical infrastructure protection for the information sector. Much of its work has been to build a framework, policies, relationships, and programs for CIP, and as much as possible the NISC looks to other nations' efforts to absorb lessons learned appropriate for Japan. In 1996 Japan adopted most policies developed in the U.S. on information security. However as the U.S. further developed its policies optimized to America's legal framework, industries, and industry-to-government relationships, various aspects were no longer appropriate for Japan.

In Japan, various sectors operate with systems of multiple standards, something quite different from the U.S. Information communications and financial systems are relatively standard; however Japan has many infrastructure systems that are not. This non-standard environment complicates development of national information security strategy. Nonetheless, Japan is an environment where systems have developed on various platforms, networks, and power systems. Proprietary designs and optimization to local factors propelled development of various systems creating this non-standard environment. Rail is an example of how regional systems developed optimizing local practicalities. As a result regional train systems are not interoperable making approaches to protections and policies somewhat complicated. In the case of local trains, contractors and local areas developed various systems tailored and optimized to specific lines and operators, precluding interoperability. Kintetsu rail in Kansai, Hankyu rail in Hanshin, and Keihan each have unique operating systems based on different philosophies. Interoperability and connectivity is not simple. Another non-standard sector is power supply. Kansai and Kanto developed power systems from different sources and times, resulting in two different hertz systems and plants that are tailored to each site and operator.

Despite a variety of standards in various systems, CIP optimization across different

sectors is important. Industries, consumers, and governments develop consensus approaches to security. NISC facilitates this work.

Responding to a crisis and recovering from its aftermath is another key area for NISC. The NISC must also develop a comprehensive picture of the developing situation and be able to present this to the Cabinet and Prime Minister for their guidance and directives.

Managing CIP from the NISC perspective addresses four primary areas. First the NISC establishes rules, guidelines, and standards. Second, it facilitates information sharing between government and industries, and various sectors of infrastructure. Third, conducts analysis of various interdependencies. NISC has a task force comprised of various specialists to understand threats and countermeasures as they relate across industries and sectors. Finally, NISC establishes and conducts cross sectional drills and exercises, an area where NISC is at its incipient stage.

Mr. YOSHIDA, Teruyoshi: Security Controls for the Financial Industry

The Center for Financial Industry Information Systems (FISC)⁶ is a nonprofit organization formed in 1984 with the authorization and approval of the Ministry of Finance. FISC is supported by 662 corporate members from a variety of sectors to include banks, insurance companies, security corporations, credit companies, computer manufacturers, system integrators, and telecommunications companies.

When initially formed, FISC emphasized its work on maintaining stability in financial operations. FISC's objective has evolved over time and it now focuses on security of financial operations. FISC promotes information security for financial industry by establishing guidelines and manuals, and raising awareness on methods to protect information security. The organization published guidelines for the financial institutions on computer systems, information systems, security policy, and contingency planning. FISC also conducts research and analysis on diverse topics related to financial information systems. It also exchanges information and perspectives on financial information systems throughout its organization.

FISC's addresses three areas of computer security in its guidelines: facility protections and emergency measures; operational security measures for management of policy, organization, assignment of responsibilities, education, and computer processes; and technical guidelines to improve system reliability, and to protect hardware and software components.

The guidelines created by FISC are reviewed and updated, managed by the FISC's Security Committee and working group. This body is comprised of experts from financial institutions, computer manufacturers, telecommunications, academia, and legal firms.

⁶www.fisc.or.jp

Mr. ARIMURA, Koichi: Topics form Telecom-ISAC Japan

Japan's Telecommunication Information Sharing and Analysis Center (Telecom-Isac)⁷ was established in July 2002 whose members collect, analyze, and share information, and take other measures to ensure stable operations in the world of telecommunications. Telecom-Isac conducts exercises to train and analyze approaches to secure telecommunications operations. Telecom-Isac operates conceptual concept of 3 "C"s: communications and collaboration among carriers, and contributions to protect the service.

Telecom-Isac has been coordinating the preparations, and executing a multiyear Cyber Attack Exercise. The exercise includes 13 organizations with a duration from 2006 through 2009; each year's exercise iteration is 10 days. It is promoted by the Minister of Internal Affairs and Communications, and three year 06-09 project. The goal of this exercise is to strengthen the telecommunications industry's capability to deal with cyber attacks. It aims to do this by presenting a cyber attack exercise on the telecommunications industry, building telecom cooperation to respond to cyber attacks, establishing a common awareness of this type of exercise, establishing a firm knowledge of the technologies involved, and developing the human resources to support the industry in the context of cyber threats and telecommunications countermeasures.

Telecom Isac also supports telecommunications capability for engineering of protection, technical operation, analysis, and response (CEPTOAR). The purpose of this sector's CEPTOAR is to improve preparedness, isolation, and recovery of IT malfunctions through cooperation among its members. It also distributes information from government or other sector CEPTOARs to its members. The Telecom CEPTOAR works with NISC at the central government and maintains a steering committee which coordinates its efforts among subordinate groups, comprised of telecom infrastructure; telecom companies addressing related services such as ADSL; ISP companies; and mobile service providers.

Ms. ITO, Yurie; JPCERT/CC CIIP efforts: Watch and Warning

Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)⁸ The organization coordinates with network service providers, security vendors, government agencies, as well as the industry associations. As such, it acts as a "CSIRT of the CSIRTs" in the Japanese community. In Asia Pacific region, JPCERT/CC helped form APCERT (Asia Pacific Computer Emergency Response Team) and provides a secretariat function for APCERT. Globally, as a member of Forum of Incident Response and Security Teams (FIRST), JPCERT/CC coordinates its activities with the trusted CSIRTs worldwide. JPCERT/CC is a not for profit, non-governmental organization which began in 1992. It is funded by the Ministry of Economy, Trade and Industry (METI).

⁷www.telecom-isac.jp

⁸www.jpCERT.or.jp

fosters the establishment of a new CSIRT and collaboration among CSIRTs; gathers and disseminates technical information on computer security incidents and vulnerabilities and security fixes, and other security information, as well as issue alerts and warnings; provides research and analysis of computer security incidents; conducts research on security related technologies; and increases awareness and understanding of information security and the technical knowledge through education and training.

Closing Session:

This session was used to discuss possibilities for the next CIP Forum. Several raised the integration and security of SCADA systems as an area that should be more fully addressed in the next session. It was noted that SCADA systems are becoming more vulnerable, effect everyone's daily lives, and are integrated into several other infrastructure systems.

The Tokyo American Center had kindly supported this conference and though the TAC could not commit to a schedule for next year, expressed their continued support to this program. National Defense University in Washington, DC was also raised as a possible future venue.

Dr. Auer thanks the organizers, presenters, and those who supported the conduct of the CIP Forum this year. He especially thanks the Tokyo American Center; the translators for their excellent work; Cwell for organizing the Forum; and financial sponsors NTT, JR Tokai, Microsoft, Mitsubishi Shoji, and Cwell.