NATIONAL INFRASTRUCTURE ADVISORY COUNCIL (NIAC)

MEETING AGENDA

Tuesday, October 9, 2007
1:30 – 4:30 p.m. EDT
National Press Club
529 14th Street NW
Washington, D.C. 20045

I. OPENING OF MEETING

Nancy Wong, Designated Federal Officer (DFO), National Infrastructure Advisory Council (NIAC), Department of Homeland Security (DHS)

II. ROLL CALL OF MEMBERS

Nancy Wong

III. OPENING REMARKS AND INTRODUCTIONS

NIAC Chairman *Erle A. Nye*, Chairman *Emeritus*, TXU Corp.

Michael Chertoff, Secretary, DHS

IN ATTENDANCE BUT DID NOT MAKE OPENING REMARKS:

Robert Jamison, Acting Under Secretary for National Protection and Programs, DHS

Robert B. Stephan, Assistant Secretary for Infrastructure Protection, DHS

Thomas P. Bossert, Senior Director for Preparedness Policy, Homeland Security Council

Neill Sciarrone, Director of Protection and Information Sharing Policy, Homeland Security Council (HSC)

IV. DISCUSSION ON INFORMATION SHARING

Ambassador Thomas E. McNamara, Program Manager of the Information Sharing Environment (ISE), Office of the Director of National Intelligence (ODNI)

V. APPROVAL OF JULY MINUTES

NIAC Chairman *Erle A. Nye*

VI. WORKING GROUP PRELIMINARY FINDINGS	NIAC Chairman *Erle A. Nye* Presiding
A. CHEMICAL, BIOLOGICAL, AND RADIOLOGICAL EVENTS AND CRITICAL INFRASTRUCTURE WORKFORCE	*Chief Rebecca F. Denlinger,* Fire Chief, Cobb County, Georgia Fire and Emergency Services, NIAC Member; *Martha H. Marsh,* President and CEO, Stanford Hospital and Clinics, NIAC Member; and *Bruce A. Rohde,* Chairman and CEO Emeritus, ConAgra Foods, Inc., NIAC Member
VII. WORKING GROUP UPDATES	NIAC Chairman *Erle A. Nye* Presiding
A. THE INSIDER THREAT TO CRITICAL INFRASTRUCTURES	*Edmund G. Archuleta*, General Manager, El Paso Water Utilities, NIAC Member, and *Thomas E. Noonan*, General Manager, IBM Internet Security Systems, NIAC Member
VIII. NEW BUSINESS	NIAC Chairman *Erle A. Nye*, NIAC Members
IX. CLOSING REMARKS	*Robert Jamison,* Acting Under Secretary for National Protection and Programs Directorate (NPPD), DHS *Robert B. Stephan,* Assistant Secretary for Office of Infrastructure Protection (OIP), DHS
X. ADJOURNMENT	NIAC Chairman *Erle A. Nye*

MINUTES

NIAC MEMBERS PRESENT IN WASHINGTON:

Mr. Edmund G. Archuleta; Dr. Craig R. Barrett; Mr. Alfred R. Berkeley, III; Lt. Gen. (ret.) Albert J. Edmonds; Hon. Tim Pawlenty; and Mr. Gregory Peters.

NIAC MEMBERS ATTENDING VIA CONFERENCE CALL:

Mr. Erle A. Nye; Chief Rebecca F. Denlinger; Chief (ret.) Gilbert G. Gallegos; and Mr. Bruce Rohde.

MEMBERS ABSENT:

Mr. George H. Conrades; Ms. Margaret E. Grayson; Commissioner Raymond W. Kelly; Ms. Martha H. Marsh; Mr. Thomas E. Noonan; Mr. James B. Nicholson Dr. Linwood H. Rose; and Mr. John W. Thompson.

SUBSTANTIVE POINTS OF CONTACT PRESENT IN WASHINGTON:

Ms. Ellen A. Black (for Chief Rebecca F. Denlinger); Mr. Bill Muston (for Mr. Erle A. Nye); and Mr. Jason Rohloff (for Gov. Tim Pawlenty).

SUBSTANTIVE POINTS OF CONTACT ATTENDING VIA CONFERENCE CALL:

Mr. Peter Allor (for Mr. Thomas E. Noonan); Mr. Scott Blanchette (for Ms. Martha H. Marsh); Mr. Andy Ellis (for George H. Conrades); Ms. Joan S. Gehrke (for Mr. James B. Nicholson); and Lt. Paul Mauro (for Commissioner Raymond W. Kelly).

OTHER DIGNITARIES PRESENT:

Michael Chertoff, Secretary, DHS; Ambassador Thomas E. McNamara, Program Manager of the ISE, ODNI; Robert Jamison, Acting Under Secretary for NPPD, DHS; Col. Robert B. Stephan, Assistant Secretary, OIP, DHS; Mr. Thomas P. Bossert, Acting Senior Director for Preparedness Policy, HSC; Ms. Neill Sciarrone, Director, Protection and Information Sharing Policy, HSC; and Ms. Nancy J. Wong, DFO, NIAC, DHS.

I. OPENING OF MEETING

Nancy Wong, DFO, NIAC, DHS

Ms. Nancy J. Wong introduced herself as the DFO for the NIAC. She welcomed Secretary Chertoff; Ambassador Thomas E. McNamara, Program Manager of the ISE, ODNI; Robert Jamison, Acting Under Secretary for NPPD, DHS; Col. Robert B. Stephan, Assistant Secretary for Infrastructure Protection, DHS; Mr. Thomas P. Bossert, Acting Senior Director for Preparedness Policy, HSC; Ms. Neill Sciarrone, Director, Protection and Information Sharing Policy, HSC; Mr. Erle A. Nye, NIAC Chairman; all NIAC Council members and members' staffs present or on the teleconference; other Federal government representatives, as well as members of the press and public. She reminded the members the meeting was open to the public and, accordingly, members should remember to exercise care when discussing potentially sensitive information. Pursuant to her authority as DFO, Ms. Wong called to order the NIAC's 21st meeting and the final meeting of 2007.

II.	**ROLL CALL**	*Nancy Wong,* DFO, NIAC, DHS

After bringing the meeting to order, Ms. Wong, called roll.

III.	**OPENING REMARKS AND INTRODUCTIONS**	NIAC Chairman, *Erle A. Nye*, Chairman Emeritus, TXU Corp.

Chairman Nye thanked Ms. Wong and thanked everyone for attending. He apologized for having to attend via teleconference. He noted the Council continued making progress and has two pending reports. The working groups would be discussing new projects at this business meeting. The Council recently met with President George W. Bush on September 21. The President is excited about the NIAC's current studies and he values the Council's work. Chairman The NIAC charter's recent extension continues the Council's operation through September 2009, something the NIAC should consider when deliberating upon future projects. Chairman Nye asked Mr. Berkeley to be prepared to assist with the meeting moderation in case there are any technical difficulties with the conference lines.

Chairman Nye thanked Secretary Chertoff for dialing into the meeting despite his busy schedule. The Secretary exhibits a remarkable degree of interest in the Council's work; the NIAC greatly appreciates this. Mr. Nye thanked Acting Under Secretary Robert Jamison, Assistant Secretary Robert Stephan, Mr. Thomas P. Bossert, Ms. Neill Sciarrone, as well as Ambassador Thomas McNamara for being present at the meeting.

Secretary Chertoff welcomed everyone and commented the NIAC meeting with President Bush was highly productive and interesting for both the Council and the President. The President and he have taken to heart the concerns the NIAC had mentioned regarding cyber threats. Additionally, the President and the Secretary will be interested in the current NIAC studies: 1) *Chemical, Biological, and Radiological Events and Critical Infrastructure Workforce* and 2) *The Insider Threat to Critical Infrastructures.* The Council's advice aided compiling strategies and plans for dealing with threats to the critical infrastructure environment. Secretary Chertoff thanked the NIAC for its participation and apologized for being unable to stay for the remainder of the meeting. He anticipated working with the NIAC in the months to come.

Chairman Nye thanked Secretary Chertoff for his interest in and support of the Council's work.

IV.	**DISCUSSION ON INFORMATION SHARING**	*Ambassador Thomas E. McNamara,* Program Manager of the ISE, ODNI

Chairman Nye noted Ambassador McNamara served eight Presidents over four decades. Though he had retired in 1998, the Department of State asked him to return following the 9/11 attacks as its Senior Advisor for Counterterrorism and Homeland Security. President Bush designated Ambassador McNamara as the Information Sharing Environment's (ISE) Program Manager, as established by the Intelligence Reform and Terrorist Prevention Act of 2004. He brings an extensive background in national security, geopolitical matters, and counterterrorism to that position. The Council anticipated Ambassador McNamara's presentation at the meeting. The

private sector maintains a continued interest in sharing information between the intelligence community and critical infrastructure owners and operators. This topic represents an underlying theme of NIAC work. Information sharing is a challenge as the government and private sector entities have varying cultures. Another such challenge is the distribution of information that may be classified. In July 2006, the NIAC completed a major report on information sharing entitled *Public-Private Sector Intelligence Coordination*. Former Council Vice Chairman and President and CEO of Cisco Systems Inc. John T. Chambers and retired Albuquerque, New Mexico Police Chief Gilbert G. Gallegos headed the study along with significant help from Chairman and CEO of Pipeline Trading Systems LLC and former Vice-Chairman of NASDAQ Mr. Alfred R. Berkeley, III and a team of subject matter experts. The report garnered high praise for its recommendations, several of which Federal entities have since implemented. Chairman Nye introduced Ambassador McNamara adding the Council looked forward to hearing his perspective and comments.

Ambassador McNamara thanked Chairman Nye for his introduction and the opportunity to address the NIAC. He stated he wanted to discuss some of his office's work over the past several months. ISE took many of the recommendations from the Council's *Public-Private Sector Intelligence Coordination Report and Recommendations*. In December 2005, the President issued a memorandum for executive department and agency heads outlining guidelines and requirements supporting ISE. Since 9/11, significant counterterrorism and information sharing improvements resulted in the creation of many government institutions and organizations. The Federal officials present at the NIAC meeting represented some of these institutions, including the:

- Homeland Security Council,
- Office of the Director of National Intelligence (ODNI),
- National Terrorism Center,
- Terrorism Screening Center,
- FBI's Homeland Security branch, and
- DHS.

State and local organizations have made considerable progress. First, the establishment of nationwide, regional, and state communications network of intelligence fusion centers represents one of these steps. Every state and major city has established or is planning to develop one of these centers. This signifies a tremendously important institutional development for the nation and its ability to share intelligence and other information beyond the Federal government. Second, Governors of various states assigned Homeland Security Advisors. While these positions did not exist prior to 9/11, there has been a significant increase in the authority and capability of the homeland security advisors in the past year. Lastly, the presence of the FBI and DHS at the state level and in urban areas continues to expand.

The government must accomplish more. The Ambassador intends to work with the Federal, state, local, and tribal government as well as private-sector partners to build on the progress made over the last six years to establish the policies, business processes, standards, and technical

capabilities allowing information management at all government levels. The government must do this in a manner protects Americans' privacy and legal rights, both individual and corporate.

The U.S. made substantial progress in implementing policies since the NIAC produced its report last year. First, the President's guidelines identified building the relationship of information movement, management, and sharing between the Federal government and the private sector. The ISE solicited considerable amounts of information from the private sector via such sources as the critical infrastructure partnership, Critical Infrastructure Partnership Advisory Council (CIPAC), the U.S. Chamber of Commerce, the Homeland Security Advisory Council (HSAC), the FBI's Information Sharing Initiative, the International Association for Chiefs of Police, the National Sheriff's Association, and the Governor's Association. ISE has been in contact with many of the major partners that play significant roles in the information sharing environment. The nation has improved coordination at the Federal level through the establishment of the National Counterterrorism Training Center (NCTC) and through the new Interagency Threat Assessment Coordination Group that will coordinate the production and dissemination of federally coordinated information from all the Federal agencies. ISE formatted this information in such a way specifically designed to be useful to state, local, and private sector partners. The ISE is intent on improving collaboration at the community level through the establishment of a national integrated network of state and major urban area fusion centers. The challenge here is incorporating the private sector into the process. These centers will be the main, but not exclusive, focus within state and urban regions for receiving, developing, and sharing counterterrorism information with each other and with the Federal government. The Ambassador expects not only an outflow from the Federal government, but also an inflow from the state and local level via the fusion centers that will produce a product that is useful on the Federal level. These centers will become the critical nodes that will make the ISE a nationally functioning institution. The ISE hopes to improve information sharing with the private sector by leveraging ongoing efforts including groups in the infrastructure sector partnership. They are working through OIP to leverage the advisory structure to engage in deliberative discussions to incorporate the private sector CI/KR and other private sector needs and capabilities into the planning processes. The NIAC remained instrumental in this advisory structure being established and congratulated the Council on their work.

The President's memorandum also mentioned standardizing a system for managing controlled but unclassified information (CUI), a new way of handling CUI requiring the needs and advice of the private sector. The lack of a standardized and simplified regiment for handling information hinders information sharing. ISE patterned the CUI framework on the existing classified system. They designed this framework to be easy for the user to understand how the system functions. As of now, the government handles CUI on a department-specific basis. If the system is standardized, every one can be sure the government handles information in a manner consistent across all departments. As for simplifying the process, ISE conducted a survey finding 107 different markings placed on controlled documents. The new system will have approximately six or less of these markings and handles information the same way across the system. This new CUI framework will be enormously beneficial.

Ambassador McNamara hoped to incorporate the needs of the private sector into the ISE. The critical infrastructure owners and operators gather, process, analyze, and share information in an effort to maintain their companies' resiliency and protect their assets, employees, and infrastructure. The private sector owns or manages a large percentage of the nation's critical infrastructure. Business owners spent years establishing strong working relationships with state, local, and Federal law enforcement and other entities; the ISE plans to leverage and acknowledge those relationships. Sharing information within the sector-specific framework has proven instrumental. Business owners tend to share time-sensitive information with government officials and other business entities within their region, but some businesses prefer to share such information based on their regulatory environments. Businesses operating on an interstate basis such as rail, communication, or within the financial sectors often prefer the business sector approach. As the ISE works to standardize its processes, it will logically account for and incorporate all the different models.

Despite significant information-sharing achievements, the nation still has an enormous amount to accomplish. Enhancing information sharing and cooperating in an effort to establish trusted partnerships remains a national priority. With trust, technology and methodology employed is all that limits sharing. The Ambassador thanked the Council for their attention.

Chairman Nye said the Ambassador's comments were helpful and thanked him for presenting to the Council. Trust represents a major challenge to overcome on both sides. He understands the perspective of both the intelligence community and the private sector. While some sectors progressed faster than others, he asked if any specific sector needed more attention to adapt to this new framework.

Ambassador McNamara pointed out the banking and financial sector began operating as an information sharing entity even before 9/11. While some may think information sharing environments signify a new phenomenon, many witness this environment every time they use an ATM or bank. The banks control shared information so each individual obtains the usable information needed in that environment. ISE hopes to utilize this model for terrorism. He lauded the banking and finance sector for their work and added other sectors continue progressing. He specifically noted the vast improvement made by the transportation as well as the chemical sectors since 9/11.

Assistant Secretary Stephan believed the nation as a whole has made remarkable improvement across the board. Every sector developed some form of information-sharing network since 9/11 by leaning on the trusted partnerships fueling this development.

Chairman Nye said industries with a business requirement to coordinate with each other and highly consolidated industries tended to be ahead in developing these partnerships. Numerous and independent businesses operating within a sector presents the greatest challenge.

Assistant Secretary Stephan agreed with the Chairman's comments. The electricity as well as the oil and gas sector had the least amount of challenges as business enterprise networks were already in place. The commercial facilities sector has made notable progress despite its numerous

diverse entities. Through the Information Sharing and Analysis Center (ISAC), these sectors have developed information sharing bridges that have served to unite varied elements into one mechanism. Every sector has at least a core minimum; now it is a matter of building upon them and ensuring to test these systems. DHS will test these in the following week with TOPOFF-4.

Chairman Nye thanked Assistant Secretary Stephan for his comments. He asked if any of the Council members had any comments.

Chief Gallegos expressed gratitude to the Ambassador on his work. Fusion centers expanded the necessary cooperative relationships. The Ambassador has helped in making substantial changes to improve those relationships.

Chairman Nye agreed with Chief Gallegos' comments and asked if anyone else sought to comment.

Mr. Berkeley said working together to address problems develops trust. He hoped the ISE both in the geographic implementation through the fusion centers and in the sector implementation through the Sector Coordinating Committees (SCCs) would find a way to frequently share information. Fueling trust is most critical during an emergency.

Ambassador McNamara concurred with Mr. Berkeley. These dialogues just started and already produced many process and problem solving changes. While developing the CUI framework, the ISE encountered several problems in private-sector arrangements with different departments of the Federal government. Thus, the ISE inserted a special clause in its framework to allow those arrangements to continue. It adjusted the framework to account for arrangements and other needs of the private sector without complicating the framework. The ISE will continue to consider those needs with this project. Through this method, they will build trust on both sides for handling information.

Chairman Nye added developing these relationships benefits both sides. The Chairman thanked the Ambassador for his work to enhance the exchange between the private sector and the intelligence community. As Ambassador McNamara committed himself to this cause, the Chairman said the industry also sought to enhance this partnership.

V.	**APPROVAL OF JULY 10, 2007 MINUTES**	NIAC Chairman, *Erle A. Nye*, Presiding

Chairman Nye preceded to the review of the July 10, 2007 NIAC Meeting Minutes. He asked the Council for any changes or additions to the minutes. The members voiced no corrections or comments. The Council moved to approve the minutes and a member seconded the motion. The Council unanimously approved the minutes.

VI.	**WORKING GROUP PRELIMINARY FINDINGS**	NIAC Chairman, *Erle A. Nye* Presiding
	A. CHEMICAL, BIOLOGICAL AND RADIOLOGICAL EVENTS AND CRITICAL INFRASTRUCTURE WORKFORCE	*Chief Rebecca F. Denlinger*, Fire Chief, Georgia Fire and Emergency Services, NIAC Member; *Martha H. Marsh*, President and CEO, Stanford Hospital and Clinics, NIAC Member; and *Bruce A. Rohde*, Chairman and CEO Emeritus, ConAgra Foods, Inc., NIAC Member

Chairman Nye introduced the *Chemical, Biological and Radiological (CBR) Threats and the Critical Infrastructure Workforce* Working Group currently chaired by Ms. Martha Marsh, Chief Rebecca Denlinger, and Mr. Bruce Rohde. The Working Group will present its findings from the radiological component of their study. The Chairman expects a completed report by the January 8, 2008 NIAC business meeting.

Study Group co-chair Mr. Scott Blanchette provided the Council with the Study Group update. He opened by saying this study is of significant length, the group has been moving forward with each of the study's three parts. The group has had the benefit of receiving outstanding contributions thus far.

Mr. Blanchette confirmed the Study Group just completed the Radiological portion of its study. The working group will present a final consolidated deliverable including final chemical, biological, and radiological reports at the January NIAC business meeting.

The Study Group's objective was to propose recommendations to the working group preparing those working in and maintaining critical infrastructure for a radiological event. The Study Group will also assess if those workers have the tools, training, and equipment necessary to identify, respond to, and recover from a radiological event.

The Study Group incorporated guidance from the White House and DHS to formulate six key questions to address in this study:

1) Do organizations have employee awareness, preparedness, and response training programs?
2) Is there market incentive to invest in radiological preparedness and response programs?

3) Is there sufficient communication infrastructure in place to respond to a radiological event?
4) What tools and technologies currently support radiological response capabilities?
5) Is there sufficient coordination between Federal, State, local, and private sector entities?
6) What can the Federal government do to encourage or facilitate enhanced preparedness and response capabilities across and between the public and private sectors?

Organizations contributing to the group outside the typical sector representation include:

- Federal Bureau of Investigation
- Georgia Army National Guard
- Johns Hopkins University
- National Defense University
- Nuclear Energy Institute
- Texas A&M University
- University of Alabama, Birmingham

Sectors represented in the context of the study:

- Chemical
- Communications
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Healthcare
- Information Technology
- Oil and Gas
- Nuclear
- Transportation
- Water and Wastewater Management

In regards to scope, the likelihood of a low-yield, dispersal device, or dirty bomb scenario represented a much more likely scenario than a traditional, nation-state, nuclear weapons attack, and thus focused on the former. In addition, DHS is concurrently undertaking a study to develop threat and vulnerability data and to refine probability scenarios. The Study Group did not want to overlap the two studies. The Study Group drew its findings from:

- Planning and preparedness
- Communications
- Training and education
- Psychological effects
- National Council on Radiation Protection and Measurements (NCRP)

- National Defense University radiological event studies
- National Response Framework
- 9/11 Commission Recommendations
- TOPOFF 4

The Study Group benefited from a body of research by the National Defense University where they pulled hundreds of individuals involved in radiological events including first responders, the Federal government, and the private sector to produce a valuable study. The first thing the study concluded was time is of the essence with accurate information needed quickly to save lives and manage fear. Second, State/local participants will look to Federal Government for information on radiation effects. Responders want information in advance, in field-useable form. Third, many participants did not know which Federal agency was principal repository of nuclear effects expertise. It is unclear which Federal officials are in charge of response. Fourth, any government participants, particularly State/local officials, stressed the need to solicit views of key private sector entities such as public utilities. Lastly, the study looked at the psychological impacts as a greater threat than actual physical damage. Radiation is the scariest effect of a nuclear attack or dirty bomb as its effects are widely misunderstood. The precedent of an initial terrorist attack will also heighten fears of future attacks. This fear will impose heavy burdens, especially on the worried-well, residents of other cities, and on the marketplace. Psychological impact of radiation will also create other down-stream negative effects, including radiation-centric treatment of victims with trauma. The findings regarding the psychological impact of a radiological event were the key finding from the study. In a low yield radiological scenario, the psychological trauma would be more significant than the actual bomb itself.

A study from Brazil examined a scenario in which 100 grams of radiotherapy waste was uncovered after 260 people were exposed resulting in four deaths and forty-nine individuals requiring medical treatment. Consequently, 112,000 people sought medical treatment believing the uncovered waste had exposed them to radiation. These people displayed symptoms that mimicked actual exposure yet were merely psychological. The group discovered in regards to psychological effects of an event that disasters may create significant impairment in 40-50% of those exposed and about 50% of disaster workers are likely to develop significant distress. Terrorism is likely to adversely affect the majority of the population, potentially between 40-90% with more psychological casualties than physical.

The National Council on Radiation Protection and Measures produced two reports, NCRP Report No. 138 “Management of Terrorist Events Involving Radioactive Material” from October 2001 and NCRP Commentary No. 19 “Key Elements of Preparing Emergency Responders for Nuclear and Radiological Terrorism” from April 2006. These reports address:

- Definition of a problem
- Roles and responsibilities
- Handling psychosocial impacts
- Medical issues of concern
- Allowable exposure
- Clean-up

- Equipment requirements for first responders; perimeter establishment and management
- Portable and stationary decontamination equipment and medical supplies
- Content and frequency of training for first responders; on-scene management

The Study Group sited these reports in regards to the accomplished in the nation's planning, preparedness, and response capabilities.

DHS released the National Response Framework for review on September 10, 2007. The framework was still in the 30-day comment period. The objectives of the report include a focus on response and short-term recovery; a consideration of all-hazards scenarios including chemical, biological, and radiological events; and the need to inform responders and emergency managers, outlining operating structures and tools. The framework addresses a number of radiological annexes including threats and vulnerabilities such as radiological dispersal devices, improvised nuclear devices, nuclear facility accidents, lost radioactive material, and transportation accidents with domestic and foreign nuclear weapons. It also provides planning and guidance including operational concepts, specifies Federal roles and responsibilities, identifies protocols for communications including resource coordination and notification, and incorporates flexibility in response approaches based on events.

The 9/11 Commission Act of 2007 provides context and framework for radiological events. Title V, Section 501 of the act discusses strengthening the security of cargo containers. It permits a container to enter the United States, either directly or via a foreign port, only if the container into and out of the United States is 1) scanned for radiation, density, and atomic elements; and 2) secured with a seal to detect and identify the time of any container breach. It also encourages the Secretary to promote and establish international standards for container security with foreign governments and international organizations. These measures should limit our exposure to certain events and threats.

DHS scheduled TOPOFF 4 for the week following this meeting. They expected the exercise to have a large number of participants with 15,000 people including some representatives from foreign countries. The Department geographically dispersed the exercise in areas such as Arizona, Oregon, and Guam. The first goal of the scenario is prevention by testing the handling and flow of operational and time-critical intelligence between agencies to prevent a terrorist attack. Second is intelligence investigation by testing the handling and flow of operational and time-critical intelligence between agencies prior to, and in response to, a linked terrorist incident. Third is incident management. It will test the full range of existing procedures for domestic incident management of a terrorist weapon of mass destruction event. It will also improve the top officials' capabilities to respond consistent with the NRP and NIMS. Forth is dispensing public information. TOPOFF4 will be a practice the strategic coordination of media relations and public information in the context of a terrorist weapon of mass destruction event or incident of national significance. Lastly is evaluation. It will identify lessons learned and promote best practices. While the results from TOPOFF 3 were not readily accessible, the Council would have hoped to have access to the lessons learned, findings, and recommendations from that event that would have been useful for the study. The Study Group would be able to incorporate some of the findings from TOPOFF 4 into the group's final report.

The Study Group had identified some deployments of surveillance and response technologies for first responders and those in proximity to likely event. Both the public and private sector have deployed a number of these. There is a fifty to sixty year history dealing with radiological threats that has supplemented the availability and distribution of sensor technology. This includes the Toxic Exposure Surveillance System (TESS) operated by CDC with American Association of Poison Control Centers to provide a real-time national surveillance and exposure database. In addition, the National Incident Management System (NIMS) operated by DHS and FEMA provides a unified incident management approach; standard command and management structures; and emphasizes preparedness, mutual aid, and resource management. Electronic sensor capabilities in the public sector include several well-equipped organizations across the country but there are limitations on the distribution and penetration of those units. The private sector does have limited pockets of capabilities including nuclear sector capabilities that responders could task to support critical event response. There is also the Community Hazards Emergency-Response-Capability Assurance Process (CHER-CAP) operated by DHS and FEMA that provides readiness, planning, preparedness, and response coordination.

Communications is a progressively developing area. Police, fire, and EMS are continually improving their communication capabilities. One example includes a DHS Report from December 8, 2006 on incident response communications interoperability. It looked at 22,400 randomly selected police, fire, and EMS agencies and studied cross-jurisdiction interoperability outpacing Federal to state or state to local interoperability progress. Another example, SAFECOM, DHS established to provide research, development, testing and evaluation, guidance, tools, and templates on interoperable wireless emergency communications. The WARN Act addresses improvements to emergency communications and provided some insights to the study. In regards to the FCC, the Study Group looked at the Communications Security, Reliability, and Interoperability Council (CSRIC) as well as the 9/11 Act's vulnerability assessment of the Nation's critical communications and information systems infrastructure and evaluation of the technical feasibility of creating a back-up emergency communications system that complements existing communications resources.

Another resource supplementing the Study Group's efforts is a sophisticated and well-organized Sector Coordinating Council (SCC). The SCC remains attuned to not only radiological event identification, but also response. The Study Group found capabilities in the nuclear sector DHS could leverage to pursue improving public-private partnership. DHS could take advantage of those capabilities in the private sector deployable in a response scenario. The Nuclear Sector Coordinating Council (NSCC) is an overarching private security entity for all phases of the Nuclear Cycle, and radioactive materials. The NSCC covers reactor operations, medical and industrial radioisotopes, research and test reactors, spent fuel storage sites, as well as transportation. The Nuclear Sector possesses inherent strengths against RDD or other potential threats posed by ionizing radiation. It has a mature science and technology infrastructure and well-established practices for working safely with radiation. Business dealing in the nuclear sector operates around the clock with robust security and health physics as well as radiation protection expertise and material controls.

The Nuclear SCC is a mature organization doing significant work assessing threats as well as creating probability scenarios and modeling. The SCC also provides oversight to radiological issues. The Nuclear sector has focused on analyzing radiological threats, including RDD threats, considering both prevention and response. They are working with industry and governmental organizations such as Health Physics Society, American Nuclear Society, National Council on Radiation Protection, Nuclear Energy Institute, Department of Energy, Nuclear Regulatory Commission. The sector was one of the largest contributors to the NCRP Report # 138, which offers a comprehensive road map for managing most aspects of managing an RDD type event. The Nuclear sector has also completed a significant amount of work in understanding the public communications dimension of an RDD event. They perform regulatory oversight in all critical elements of the business including developing a deployable, trained, organized emergency response infrastructure. The sector has taken an all hazards approach to handling any emergent situation of varying degree of severity, including general radiological emergencies. They coordinate periodic training, drills and exercises, including jointly drilling with public sector first responders.

DHS might be interested in how to engage the nuclear sector in a public-private partnership in terms of bringing resources trained and knowledgeable with the tools and technologies useful in a radiological event. With some planning and efforts, they could be a key contributor to a radiological event response scenario. The nation could potentially develop and deploy training modules for all first responders by adapting existing industry training programs. It could also explore memorandums of understanding for private sector expert resource sharing during an RDD emergency, as there exists private-sector expertise in most U.S. states. In addition, the nation could leverage industry knowledge and experience in developing a credible communications strategy and assistance in tailoring messages for public release.

The country continues to accomplish outstanding work in dealing with all potential hazards. There exists a need to complete the prioritization of comprehensive, national risk assessment included in such projects as RAMCAP and NIPP that prioritizes radiological threats and vulnerabilities within context of other threats such as chemical or biological. The Study Group noticed a common theme is the question of what role does each organization play in different types of scenarios. They also emphasized the importance to defining roles and responsibilities for agencies that impact the transportation of, and accountability for, radiological materials including such agencies as Customs and Border Enforcement, the Transportation Security Administration, the Department of Transportation, the US Coast Guard, and the Nuclear Regulatory Commission. The Study Group questioned how to bring all the necessary groups together in an efficient, well coordinated, and planned scenario.

Mr. Blanchette complimented the work DHS has accomplished in regards to dealing with a radiological event. Threat scenarios continue to be modeled and simulated and such events as TOPOFF4 are bringing personnel into the field. Mr. Blanchette encouraged DHS to continue its work in planning, preparedness, and response. They are making progress in a quick and efficient manner. The Study Group suggested the continued improvement of knowledge around specific scenarios, impact, and likelihood of events. This includes assessing usability and availability of planning data, continuing to deploy tools to support planning and response scenarios, increasing

understanding of threat and vulnerability risk factors and attendant response mechanisms, and conducting regional cross-sector assessments. The Study Group also suggested the improvement of accessibility to planning and response material.

The Study Group recommends clearly defining response roles, responsibilities, and communication protocols, as there tends to be significant overlap. Response exercises such as TOPOFF4 will continue to improve planning, preparedness, and response capabilities for first responders. The nation should continue to improve accessibility and economic viability of necessary equipment, improve readiness of first responders, and continue to staff and support fusion centers.

There is substantial innovation in surveillance and detection tools and technologies. The S&T Directorate at DHS focuses on improving information collection, analysis, and reporting mechanisms that support radiological event detection. The Study Group recommended the continued funding of collaborative, public-private efforts to develop more advanced detection solutions including such labs as Idaho National Lab, Lawrence Livermore National Lab, Argonne National Lab, Brookhaven National Lab, and Los Alamos National Lab. Mr. Blanchette noted there are new technologies yet to be deployed. He added the government might consider accelerating deployment of those tools/technologies under development. This may include reducing the cost on the developer, which may be inhibiting distribution of these technologies, and identifying commercialization mechanisms making solutions more broadly available to public and private sector stakeholders.

The Study Group was encouraged by the continued progress with NIMS/NRF re-write. They found the document to be thorough, addressing radiological dispersal devices in a high degree of detail. The government should continue to address national, state, local flow chart communications and more clearly define roles and responsibilities across all levels of government and the private sector. The Study Group suggested the government continue to make strategic improvements, including implementation of the WARN Act and SAFECOM. They also recommended improving tactical event communications capabilities, specifically around first responder, private sector, and fire/EMS/law enforcement resources.

The Study Group extracted some recommendations from the National Defense University (NDU) radiological study. NDU stressed the need for early identification of impacts on key infrastructure including communications, transportation, and power. NDU also identified the need for greater understanding of the government's capacity for response and the availability of response personnel and medical resources. Knowing who is in charge of the response, what the lead Federal agency is, and what the chain of command is all are important to handling such an emergency. NDU also mentions the need for receiving timely guidance on how to respond as well as rapid delineation of radiation hazard zones. This includes defining a perimeter, its variability, and whether responders can safely enter. An improved understanding of the government's capacity on response could help in making strategic investments or develop strategic partnerships to help fill in any gaps within the response capacity. Many studies stressed the importance of knowing who was in charge of a situation.

The Study Group found a great deal of information available on nuclear effects and response. While this is not a new field of study, the threat scenarios have changed. Nation states are no longer as great of a focus as are lower yield higher probability scenarios. There is a significant amount of data available to formulate threat vulnerability scenarios. The Study Group found information is not yet adequately adapted for contemporary responders' needs. Thus, they recommended that information be adapted for use by first responders and incorporated into their education and training programs. They encountered a perception among response community that information is sparse. State and local workshop participants emphasized need for at-hand, detailed, how-to guidance, especially regarding radiation effects and response roles/responsibilities. Hurricane Katrina demonstrated shortcomings of national response, but the nation is working to address these needs. Therefore, the most important response challenges appear to concern filling knowledge gaps for effects on issues that post-date aboveground testing. In addition, making knowledge readily accessible and useable for contemporary responders, clarifying roles and responsibilities, and improving mechanisms of cooperation are also significant challenges.

The Study Group anticipates presenting a consolidated report at the January 8, 2008 NIAC meeting. Mr. Blanchette thanked everyone for their time and apologized for not being at the meeting in person.

Chairman Nye commented this report was of significant interest. The remarks Mr. Blanchette made on the psychological effects of a radiological attack do create concern for the use of a radiological device to potentially create panic. He asked while communication and information is a means of countering this threat, what did the group suggest as a means of mitigating the psychological impact of a radiological attack.

Mr. Blanchette said key communities with information to diminish the impact of this threat need to help incorporate that information into response scenarios. The nation has yet to incorporate it in a useable format into the curriculum and training of first responders. He added the group might recommend incorporating such information into the education of the nation's emergency responders.

Chairman Nye noted an unprepared and ill-equipped medical facility could be a danger equivalent to an actual attack.

Mr. Blanchette agreed and mentioned the incident in Brazil where over 100,000 healthy people believed they were sick because of a radiological event.

Chairman Nye asked if there were any other comments or question.

Governor Pawlenty asked if Mr. Blanchette could comment on the implementation of the group's recommendations, specifically adapting existing training modules and potentially partnering with the states who can heavily aid in training first responders.

Mr. Blanchette agreed the Study Group should make the structuring of the report practical for implementation. He expressed hope partners in government would take ownership of the reports recommendations and push for their implementation.

Governor Pawlenty commented the group raised some excellent issues and questions. The Governor hoped the group would effectively break down the issues into a course of action and areas of responsibility for implementation.

General Edmonds commented the group made some significant points in regards to surveillance detection technology. He suggested the group look at what is available in the private sector as the private sector has been studying radiological threats for many years. He added it would be of interest to see what the current ability is and where there are gaps to fill.

Mr. Blanchette noted one of the legacies of the Cold War was extensive equipment that the government could deploy. There are issues about the age of some of the devices that may affect their usability, but organizations such as the Army National Guard have much equipment that the country could utilize in the event of a CBR event. He predicted figuring how this could be done would be a significant challenge.

General Edmonds commented industry would most likely take the lead in developing the next generation of technology, expanding the function of devices already on the market and building upon what is already in place. The government should find out what equipment is still usable and then modernize on it.

Mr. Berkeley asked if Mr. Blanchette could address the issue of prolonged response time in simulations because of such issues as responders taking a significant amount of time to suit up.

Mr. Blanchette noted many individuals the group questioned voiced similar concerns. The psychological impact of a radiological event is significantly greater than the clinical effects. Individuals were dieing more quickly because they were concerned about the effects of radiation. This recommendation may fall under greater education and training of first responders to mitigate the perceived effects of radiation.

Hearing no more questions, Chairman Nye thanked the Working Group for the discussion. He commented he looks forward to the final deliberation of the Working Group in January.

Assistant Secretary Stephan commented the annexes of the National Response Framework are currently under a sixty-day period for public review. DHS would make available drafts of the framework to those in the public involved in emergency management to incorporate their ideas into the report and address questions such as those raised by Governor Pawlenty. DHS headquarters has an interagency planning team working through the 15 national contingency scenarios, including CBR events, who will also review the framework. DHS plans to present an updated document in January incorporating inputs they received.

Chairman Nye thanked Assistant Secretary Stephan for his comments.

VII.	**WORKING GROUP UPDATES**	NIAC Chairman, *Erle A. Nye* Presiding
	A. THE INSIDER THREAT TO CRITICAL INFRASTRUCTURES	*Edmund G. Archuleta*, General Manager, El Paso Water Utilities, NIAC Member; and *Thomas E. Noonan*, General Manager, IBM Internet Security Systems, NIAC Member

Chairman Nye introduced the Insider Threat to Critical Infrastructures Working Group chaired by Mr. Thomas E. Noonan and Mr. Edmund G. Archuleta. Mr. John W. Thompson and Ms. Margaret E. Grayson also serve on the Working Group. The Chairman expected Mr. Peter Allor would be presenting for the group.

Mr. Archuleta wished Chairman Nye and the rest of the Council a good afternoon. He expressed his pleasure to be presenting at the meeting. Mr. Archuleta pointed out Mr. Allor would be representing. Mr. Noonan and that Vance Taylor, who has been representing the water sector for this project, is also present. Mr. Archuleta added the Study Group would be presenting on less technical aspects of their study at the meeting and dealing more with psychological and social aspects of human behavior. The Council took on this study early in the year and in July provided a progress report. At this meeting, the Study Group would be presenting a summary on Phase I of the two study phases. The first phase was to identify the insider threat to critical infrastructure, including the dynamics involved, the obstacles to mitigation, and the effects of globalization. The Study Group is now prepared to move onto the second phase, which will focus on the legal, procedural, and policy barriers for private sector infrastructure operators and employee screening. Mr. Archuleta thanked Mr. Michael Schelble for the work he has done on the study. He added this was topic material is difficult to address. The Study Group will be providing information on information sharing, education, awareness, background investigations, and technology. Mr. Archuleta introduced Mr. Allor to present the summary for the Study Group. Mr. Archuleta added the Working Group would be circulating a draft report to the Council for any comments.

Mr. Allor thanked Mr. Archuleta, Chairman Nye, and the rest of the members. Mr. Allor noted the Study Group could use the help of more members. He confirmed he would be presenting the Study Group's preliminary report for Phase I of their study and will be outlining the work for Phase II.

The Study Group broke down the objectives of the study into two phases. The first phase, focused on defining the insider threat to critical infrastructures, including dynamics involved, obstacles to mitigation, and the effect of globalization, is nearly complete pending the consensus of a few points that the Study Group will be revisiting in Phase II. This next phase will build on what the Study Group learned in the first phase and focus on legal, procedural, and policy barriers for private sector infrastructure operator employee screening efforts. The Study Group expects the completion of the study may produce potential recommendations for improving

operators' ability to address the insider threat to critical infrastructures, and seek to provide guidance on a clear legal environment for operators in dealing with potentially hostile insiders.

The definition the Study Group has composed for insider threat has thus far proven to be solid. They drew from definitions produced by such groups as the Department of Defense, the Department of Justice, and the Secret Service. The Study Group defined *insider threat* in regards to critical infrastructure as:

> *an individual with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm*

One aspect important to accomplishing this first phase was identifying what the threat was. This may include the interruption of services delivery, impact to the national economic backbone, or a negative impact to public health and safety. Another important aspect for the Study Group was assessing the risk. They based this risk on the level of access an employee has to critical systems or an individual's knowledge of critical systems and vulnerabilities. These two areas of study were essential to the next phase of the Study Group's project.

The Study Group's scope utilized a risk management approach to protection based on informed understanding of threat, vulnerability, and consequence. They accomplished this by means of a thorough understanding of how a business functions. With this knowledge, one can identify and prioritize risks based on identification of critical assets. That part of understanding threats includes knowing who the actors are and what the motivations are. The Study Group stresses the importance of psychology behind an insider threat specifically the "disgruntled" insider. While there exist a large number of disgruntled employees, they do not all pose a threat. The Study Group has noticed an emerging economic espionage threat where individuals can benefit financially from competitors for their insider knowledge. They also noticed variation on maturity and awareness of the insider threat in the varying sectors.

Looking more closely at the importance of psychology and the "disgruntled" insider, a CERT/CC-US Secret Service study, which found commonalities between U.S. espionage cases and known cases of "disgruntled" insiders committing acts of IT sabotage. Understanding this issue prior to an event and developing policies to handle such situations is essential to reacting to the situation. The Study Group noticed common characteristics and common paths to betrayal within most cases. This commonality takes the form of an external stressor. If management knows what to look for, it can aid in mitigating a potential issue. Remaining attune to these factors can be the most effective means of preventing such situations.

The Study Group found variation on maturity and awareness of insider threats. Sectors heavily regulated such as financial services and the nuclear sector continues to focus on mitigating the issue. Larger sectors tend to be more prepared to deal with such threats. While certain sectors as a whole may be more prepared, smaller parts of those sectors may not have procedures in place. To effectively deal with this threat, the nation's critical infrastructure sectors need a common understanding of the risks for owner-operators. A misperception of risk can result in complacency and denial. While there may be a level of awareness, the sectors as a whole do not

fully understand the risks and potential consequences. To get CI owner-operators to actively manage insider risks, they need a common, clear understanding of the threat as well as achievable, cost effective mitigation goals. One area lacking maturity was information sharing on what is happening with insider incidents, including depth of the threat and trends. While security strategies to handle external threats are well developed, strategies to deal with internal threats are not nearly understood or followed.

Some of the dynamics of the insider threat include escalating technology and network risk in combination with globalization and a globally dispersed workforce. The Study Group saw initial screenings of employees widely practiced, but that long-term employees manifest insider threats most commonly. Technology risks for companies are growing at a rapidly escalating rate, faster than the solutions to those risks. One such example of this growing threat is the proliferation of small, mobile computing devices and constant network access that erode traditional workplace boundaries.

Globalization has had a significant effect on the insider threat issue that varies in different ways and to different degrees from sector to sector. Some of these emerging globalization risks include the expansion of trusted insiders within a company to new populations that are less verifiable and with different cultural norms. There is an increased difficulty in background checks partly due to some cultures' view on their usage. Emerging global supply chain vulnerabilities as well as legal issues may exacerbate the problem.

There are several obstacles to addressing the insider threat. Firstly, in regards to information sharing, there exists no reliable threat intelligence with any trusted entity for collection and protection of that information as well as little incentive to share information on insider incidents. Secondly, when dealing with education and awareness, there is a need for a baseline understanding of insider threats as well as a need for effective mitigation programs, which may require a cultural change within industry. Thirdly, the Study Group found background investigations were not universally accepted with any standard or common process. The Study Group suggested periodic reinvestigation or monitoring for critical positions. Fourthly, they found technology threats are growing faster than the solutions. Thus, there is a need for more deployable, adaptable solutions. Lastly, the Study Group observed in regards to cultural and organizational obstacles, there needs to be collaboration between information technology, human resource, security, and asset owners to address insider threats. One such instance of a potential threat situation is the unquestioned trust of long-time employees.

The Study Group plans to develop specific, actionable recommendations to address identified obstacles. Firstly, there needs to be a strategic level of information sharing on insider threats. Government intelligence agencies need to share relevant strategic level information on insider threats. On the other hand, the sectors need to establish a trusted process and mechanism to share incident information that protects the anonymity of the contributing organization. This may require an insider threat clearinghouse/resource for owner/operators seeking to assess and mitigate their insider risks. Secondly, the Study Group suggested an education and awareness framework. This includes an executive and workforce education and awareness of insider threats This would require a flexible methodology for senior management implementation for affecting

cultural change. Thirdly, the Study Group will be looking into developing finding and recommendations examining the challenges facing infrastructure operators in developing risk-focused background investigation programs in phase II. The Study Group has had good discussions with DHS regarding this issue and will be looking for follow-ups at a face-to-face meeting they have scheduled. Fourthly, they have been conversing with technology companies to investigate needed technology solutions for mitigating insider risks. Lastly, the Study Group will also be looking at cultural and organizational obstacles in phase II.

The Study Group has now begun phase II research and is on schedule to finalize the phase I preliminary draft report. Mr. Allor said he looked forward to the members' comments and reviews on that report. The Study Group will continue to research and develop specific, actionable recommendations for identified obstacles. Once the Study Group completes its phase II report, it will combine both phase findings into a single report for the Council's review at the January 2008 meeting.

Mr. Allor asked if there were any questions.

Chairman Nye remarked the Study Group has put a significant amount of work into this study. He added he is interested in seeing how the Study Group deals with some of the procedural, legal, and policy barriers in the second half of their study. He asked if it was reasonable to expect a final report by January.

Mr. Allor said the Study Group is aiming for January to finalize its report, but it will depend on the research and the discussions on the data drawn from that research.

Chairman Nye thanked the Study Group and asked if there were any questions or comments. He added though he looks forward to a completed report, it is better to have a thorough study than an expedited product.

VIII. NEW BUSINESS

NIAC Chairman, *Erle A. Nye*, NIAC Members

Chairman Nye moved onto new business, noting the NIAC's two ongoing studies both continue making significant strides towards final recommendations. With these two efforts nearing completion, a number of areas come to mind for potential Council studies and reports. The President expresses much interest in these subjects and remains particularly anxious to pursue areas relating to cyber security. Chairman Nye expected guidance from the White House in the following weeks on subject matter for the Council to review. He welcomed any such guidance from DHS as well. The members provided several ideas for topics, but Council needs to prioritize these ideas based on immediate importance. Mr. Muston has put together a list of topics and hoped some members would express interest in leading a Working Group. The Chairman introduced Mr. Muston to address these topics.

Mr. Muston thanked Chairman Nye for the introduction and asserted the members provided him with many good potential topics and added prioritizing these topics remains a challenge. With this, he opened the discussion of potential topics.

One issue that remains an important one is dealing with catastrophes. On several occasions over the past three years, the NIAC voiced concerns over the private sector's ability to deal with never-before-seen terrorist events. Without such experience, it seems unlikely the nation could identify actions needed for response and recovery in the wake of an incident. Catastrophic events to critical infrastructure could threaten the continuity or financial viability of those critical infrastructures, even with the restoration of the infrastructure's physical activities. This study might examine critical infrastructure owners and operators' ability to respond to an incident and restore their capabilities. Another key piece would identify the challenges to responding to an event. As well as the challenges in doing so, it may also look at limitations such as difficulties in obtaining or transporting supplies or equipment. This may include actions that might provide relief including Federal powers. This study could examine the financial consequences and the continued financial viability of organizations even after the nation restores its physical capabilities. The federal government has already put in place authorities such as the Defense Production Act, the Stafford Act, and the Terrorism Risk Insurance Act. We need to understand whether these acts represent a comprehensive framework to handle terrorist events.

The second topic Mr. Muston proposed seeks to develop a regional cooperation framework. Many states, local communities, as well as the Federal government implemented policies and procedures for dealing with natural disasters such as hurricanes. Federal critical infrastructure protection framework for critical infrastructure protection exists and includes the public-private partnership model and some states implemented similar programs. Terrorist events would likely be localized and possibly impact concentrations of critical infrastructure such as refineries, ports, and critical bridges. However, no broadly recognized critical infrastructure protection framework exists recognizing major facilities in local areas and the best approach for partnership for the facility itself including local agencies and law enforcement, state agencies and law enforcement, and Federal entities. Such a framework is needed that would address planning, preparation, information sharing, prevention, response and recovery. This topic could address the question of what improvements in a cooperative framework between local critical infrastructure and local, state, and Federal authorities including intelligence, law enforcement, and first responders would be useful.

Third, Mr. Muston raised a topic in regards to interdependencies among sectors. Interdependencies exist throughout our economy and a concern to this Council would be interdependencies among critical infrastructures. Specific sectors are especially aware of their dependencies on other sectors. This includes the movement of critical bulk materials and products and the transport of energy, among others. The Council has suggested two lines of inquiry for future studies. One asks if Sector Specific Agencies can better promote the communications and relationships between the independent sectors, so that the sectors themselves can better plan for potential consequences associated with those interdependencies. The other asks about specific interdependencies around rail transportation and whether these are so critical as to merit special consideration.

The last topic Mr. Muston addressed dealt with partnership assessment. The public and private sectors have made substantial progress in the last several years for critical infrastructure protection. HSPD-7 has established lead agencies for each critical infrastructure sector, with an umbrella role for DHS. DHS has created the National Infrastructure Protection Plan with Sector-specific elements. The private sector has established Sector Coordinating Councils in conjunction with Information Sharing and Analysis Centers. PCIS has expanded a partnership of the sectors and the Critical Infrastructure Protection Advisory Council (CIPAC) builds a public-private partnership. The NIAC has addressed elements of these in prior reports, but now may be an opportune time for the Council to step back and assess the accomplishments in both public and private sectors and in the partnership, identify opportunities for improved effectiveness, and establish a vision for the partnership that articulates its value to a larger audience. One must recognize that, in little more than a year from now, a new Administration will be in place. Such a study provides the opportunity for some self-assessment by the private sector under executive leadership of the Council, as well as assessment of the partnership with the public sector.

Mr. Muston believed these were four robust and timely topics that the Council put forward. He expressed his appreciation for the members' inputs and considerations as he found their ideas stimulating.

Chairman Nye thanked Mr. Muston. The Chairman noted Chief Denlinger was particularly interested in the topic regarding the regional cooperation framework. He added Mr. Berkeley had expressed interest in the first topic Mr. Muston had presented. He noted there has been significant discussion outside of the Council regarding the strategic plan for a private sector partnership and there has been a substantial amount of work accomplished in that area including a report from Ambassador McNamara relating to that topic. There is still work the nation can do beyond information sharing and into dealing with the issues in establishing a full partnership. Mr. Nye asked the members to express if they believed any of the four topics merit any more consideration more than the others.

Al Berkeley addressed the topic regarding dealing with catastrophes stemmed from conversations John Chambers and the Council had several years ago. It sought to answer the question of what happens when one needs an authority not available in the law. He mentioned the example of the impact to the insurance industry with an attack on a ship in the Straits of Hormuz where the insurance company backed off and went to war clauses. One of the Arab Sheiks ended up underwriting the insurance side of shipping oil. Another example Mr. Berkeley mentioned was in regards to 9/11 and the questions over closing the markets. There were very strict procedures to accomplish this, but they managed to close the markets anyways. There were also several of these contingencies in Katrina where the Federal government was unauthorized to enter the state for some time. Mr. Berkeley reiterated he would be interested in this topic because he has had some exposure through the events of 9/11.

Chairman Nye asked if there were any more comments on the topics.

Governor Pawlenty agreed with Mr. Berkeley's comments in regards to dealing with catastrophes. He commented Minnesota had recently dealt with several disasters including flooding, a drought, and a bridge collapse. He added it might be helpful to consult those government entities interested in these reports more critically. There is a lot of effort put into these reports to list out concerns and challenges. He suggested more focus on tangible recommendations by spending more time on developing scope of each report to increase the value to the government with suggestions ready to input.

Chairman Nye responded to the Governor's comments adding in some instances, the Council supplied detailed recommendations with specifics on what the nation needs to do, how it could be done, and who ought to be involved. The Federal government primarily implemented those recommendations. In other instances, the Council analyzed and compartmentalized the problem by pointing out the issues that need to be resolved and what elements may be helpful to industry. The Chairman continued nothing while some reports have been more specific than others, his experience with the White House, DHS, and others has shown getting industry's perspective on what needs to be done in itself is helpful. He agreed with the Governor that getting input from the Council's constituents is useful. Chairman Nye continued saying the topic regarding partnership assessment intends to build on a topic upon which the Council has already touched and its recommendations implemented organizationally. Now the question is on how to make that organization work and get the right people involved. The Chairman suggested the fourth topic make specific recommendations useful to both the government and private sector.

Governor Pawlenty said that as the Council seeks input, they should ask for openness and focus on a tactical level. It may be useful to narrow the scope of the topics and focusing on the aspects of a topic that are most chronic and challenging.

Chairman Nye noted the current two Working Groups had sought to narrow the scope of their topics. The radiological group had concentrated on dirty bombs rather than nuclear warheads. He commented the Governor made an excellent point. The Council is set up to deal with high-level policy issues. He commented the group is a remarkably productive group of volunteers.

Chairman Nye asked for any more comments.

Mr. Archuleta said the topic regarding interdependencies among sectors was an idea he had suggested. Such utilities as water require a lot of energy to function and vice versa. He hoped the Council would prioritize this topic as he believed it was of significant importance.

Mr. Barrett noted the topics tend to come from two different perspectives. The first being how might the nation respond to a catastrophe. The other deals with how might the nation put infrastructure in place to respond to a catastrophe. Industry tends to focus its interest on issues that could be a problem to them specifically. The more specific a topic is, the higher the interest. Mr. Barrett questioned whether the Council should focus on protection or resiliency.

Mr. Berkeley suggested posing the question to the SCCs noting specifically the events of 9/11 or Katrina and asking what the grey areas were in laws that slowed down response. Mr. Berkeley

also suggested seeing if there are any contingent legislation or regulation that could be put in place ahead of time to circumvent this problem.

Chairman Nye said this was a good point. He recommended putting more detail and focusing the topics that Mr. Muston had presented. Mr. Muston asked if there were any more comments.

Mr. Peters commented there is an emerging concern over cyber security issues. He noted an approach called Unified Communications or Communications Enabled Business Processes where there is a collapse of the physical IT infrastructure with the software world as well as a centralization of the intelligence in communications infrastructure. He believed an assessment of the emerging threat might work well with the concern over cyber security threats.

Chairman Nye said the President was pleased with the work being done, but the President did suggest moving towards cyber issues more than physical issues. He added the Council would consider this suggestion as they review the topics.

IX. CLOSING REMARKS

Robert Jamison, Acting Under Secretary for NPPD, DHS

Robert B. Stephan, Assistant Secretary for OIP, DHS

Chairman Nye asked if Assistant Secretary Stephan had any comments. He thanked the Assistant Secretary for providing the Council with copies of the Office of Infrastructure Protection (OIP) Strategic Plan for fiscal years 2008-2013. The Chairman suggested the review of the report as it gives structure to what the Council has been doing.

Assistant Secretary Robert Stephan commented that the Department put a significant amount of work into assembling the OIP Strategic Plan. The plan helps give OIP, as well as its partners from various levels of government and private sector, a better idea of the direction in which the office is heading. The plan will serve as a bridge between the current administration of George W. Bush and successive administrations. Each part of the plan addresses each of the basic functions OIP performs, including the information aggregation role, analysis role, information-sharing partnerships, and risk reduction and incident management. The plan presents a vision for the next five years based on budget levels and resource support for each individual program and for OIP as a whole.

The Assistant Secretary reiterated that OIP would focus on four principle areas of activity during the remained of the Bush administration. The first principle is implementing the National Infrastructure Protection Plan (NIPP) and Sector-Specific Plans (SSP) in concert with the private sector and State and local partners. This is paramount as many individuals came together and gave significant thought to create these work products. With the development of these products, OIP now has a timeline with concrete deliverables that it is pushing toward going forward. OIP must do everything it can in terms of implementation while remaining resilient to any emerging threats or natural disasters, the Assistant Secretary said.

The second principle on which OIP is working is to expand the ability of State and local government partners to implement the NIPP. The Assistant Secretary highlighted a homeland security advisor consortium composed of 14 States stretching from the mid-Atlantic region to New England that have been implementing the NIPP at the State and local government level. Homeland security advisors, he said, are committed to using the framework and information-sharing pieces. To date, the consortium has implemented the NIAC's recommendation to stand up advisory Councils where the public and private sectors come together at the State level. Resources were a common theme in the briefings presented at the consortium, the Assistant Secretary said. States with the ability to push certain forms of Federal grant dollars into sustainable programs have made the most notable progress and advancement toward their goals. While other States are just beginning this process, all States associated with the consortium focus on this mission to varying degrees.

Without the NIAC recommendations, none of this would be happening, Assistant Secretary Stephan insisted. The NIAC produced the recommendations that not only OIP, but also the State and local levels are implementing. These recommendations bring together private sector partners from across all Critical Infrastructure and Key Resource (CI/KR) sectors. Each of the States in the 14-State consortium has adapted the NIPP to fit its own security landscapes and to benefit the businesses operating inside their jurisdictions.

The third principle for which OIP is focusing its efforts involves closing remaining loopholes in incident management. OIP has a solid CI protection assessment resiliency annex to the national response framework under review. At present, the annex is in its 60-day comment period along with other annexes. The Assistant Secretary recommended that those individuals interested should look at those documents and help the OIP fine-tune the framework. DHS is currently operating within this framework in terms of responding to any terrorist event or natural disaster. Created with the help of the Sector Coordinating Councils (SCCs), the upcoming TOPOFF4 event will test the framework. DHS is bringing in a large number of private sector representatives for this event through the SCC structure that the NIAC helped put together. The private sector is helping DHS devise creative ways to impact each industry during the event. DHS brought the sector representatives into the scenario development process in all the planning conferences leading up to the TOPOFF4 exercise. At each of the three scenario venues, sector representatives will operate a significant white cell, a group of subject matter experts that evaluate the effectiveness of the exercise, responsible for responding to incidents chosen by the private sector entities. DHS will have at the venues private sector representatives including individuals from national corporations and members of the FCC. The white cell will provide additional input during the event. TOPOFF4 will have the widest level of private sector participation more than any prior TOPOFF exercises. As the TOPOFF project matures, DHS is capable of incorporating even greater numbers from the private sector.

The last principle focuses on OIP's efforts to build an aggressive chemical security regulatory framework that works in partnership with the Chemical Sector, as well as those elements of industry that deal with toxic chemicals of concern. The Assistant Secretary said that this would not look like the traditional safety frameworks already in place across various industries. Instead,

it will, be a collaborative security partnership that will contribute to a cooperative environment between the Federal government and private industry. This framework will allow the industry to focus its attention on real threats, such as Al-Qaeda and others who are attempting to use the nation's own chemical sector and toxic chemicals as a weapon to disrupt the U.S. economy. This is a new and unique regulatory structure with a lot of participation from State and local government and law enforcement agencies, he added.

Based on the NIAC recommendations, the OIP has activated a new State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) headed by Michigan's homeland security advisor, Colonel Michael McDaniel. DHS uses this Council to provide feedback and opinions on policy and as an implementation mechanism to garner involvement of all the various State emergency responders and emergency managers. The Assistant Secretary asked the NIAC to assist OIP implement the NIPP, the SSPs, and the chemical framework. There is not, Assistant Secretary Stephan noted, a tremendous amount of time before a new administration moves into the White House, and therefore there is not a lot of time plan for the future. Whether the next administration is Democrat or Republican is of no consequence, he said, adding that OIP will provide a set of comprehensive plans and protocols to the next administration to continue its work. In an ever evolving, generation's long battle with terrorism, Mother Nature, and other nemeses, the NIAC, the Assistant Secretary suggested, could help a new administration think about the next level to this mission and build upon the things OIP has already institutionalized, including the Sector Partnership Framework.. If the NIAC could help the next administration focus and give some timely feedback in terms of the OIP strategic plan, it would be immensely helpful, he said. DHS remains focused on fighting the near term war and those who take up this role in the next administration will need help in fighting the long-term war. The Assistant Secretary suggested that one of the NIAC's next Working Group topics might address this question. It would, he said, be of an incredible service to the nation. He offered the NIAC all the resources DHS has to offer.

Chairman Nye thanked Assistant Secretary Stephan and remarked that he always has thoughtful comments.

Mr. Berkeley asked if Acting Under Secretary Jamison had any comments he wanted to add.

Acting Under Secretary Jamison thanked the NIAC, noting that there are some important issues that need to be addressed with the transition into the next administration. Even though the Department is new in many ways, DHS has made significant progress, he said. Over the next 15 months, DHS must address transition-related issues. The perspective of the NIAC in regards to where DHS needs to be heading would be of tremendous help.

The Under Secretary added to Governor Pawlenty's comments from earlier in the meeting that the NIAC should create reports that are actionable for the government, noting that Council has accomplished notable work in this regard. The Under Secretary added that he is currently working with an advisory Council Working Group to develop policies and procedures that will provide directional guidance to keep the Council in alignment with all the other areas of its

activity. The Under Secretary offered to share with the NIAC Council any recommendation from that project.

Chairman Nye thanked Acting Under Secretary Jamison.

X. ADJOURNMENT NIAC Chairman, *Erle A. Nye*

Chairman Nye pointed out that the next NIAC meeting will be held January 8, 2008 in Washington D.C. He informed the members they should expect a final draft report from the *Chemical, Biological, and Radiological Events and Critical Infrastructure Workforce Working Group* and *The Insider Threat to Critical Infrastructure Working Group.* The Chairman requested Mr. Muston to compose a brief summary on each of the potential new topics including the topic ideas Assistant Secretary Stephan addressed. Mr. Nye noted other topic ideas are always welcome. He asked if there were any further comments from the members. Chairman Nye then thanked everyone for their participation and adjourned the meeting.

I hereby certify the foregoing minutes accurately represent the discussion and events that transpired at the meeting held on the date first noted above.

By: /S/ Erle A. Nye Dated: January 8, 2008
Erle A. Nye, Chairman

ATTACHMENT A

The Chemical, Biological, and Radiological Events and Critical Infrastructure Workforce

NIAC Chemical, Biological and Radiological Events and the Critical Infrastructure Workforce

Martha H. Marsh
President and CEO
Stanford Hospital and Clinics

Chief Rebecca F. Denlinger
Fire Chief
Cobb County, GA Fire and Rescue

Bruce Rohde
Chairman and CEO Emeritus
ConAgra Foods, Inc.

Overview

- **Working Group Process Update**
- **Radiological Objective/Scope**
- **Key Questions**
- **Contributors**
- **Findings**
- **Recommendations**

Radiological Objective

- **Provide recommendations for preparing those who work in and maintain areas considered Critical Infrastructure (CI) for a radiological event and ensure they have the tools, training, and equipment necessary to identify, respond to and recover from a radiological event.**

Key Questions

- **Question #1: Do organizations have employee awareness, preparedness, and response training programs?**
- **Question #2: Is there a market incentive to invest in radiological preparedness and response programs?**
- **Question #3: Is there sufficient communication infrastructure in place to respond to a radiological event?**
- **Question #4: What tools and technologies currently support your radiological response capability?**
- **Question #5: Is there sufficient coordination between Federal, state, local, and private-sector entities?**
- **Question #6: What can the Federal government do to encourage or facilitate enhanced preparedness and response capabilities across and between the public and private sectors?**

Contributing Organizations

- **Federal Bureau of Investigation**
- **Georgia Army National Guard**
- **Johns Hopkins University**
- **National Defense University**
- **Nuclear Energy Institute**
- **Texas A&M University**
- **University of Alabama, Birmingham**

Scope and Findings

- Scope

  - Focused on low-yield, dispersal device, or dirty bomb scenario.
  - Did not focus on traditional, nation-state, nuclear weapons attack.
  - DHS concurrently studying / developing threat and vulnerability data to refine probability and impact scenarios.

- Findings

  - **Planning and preparedness**
  - **Communications**
  - **Training and education**
  - **Psychological effects**
  - **National Council on Radiation Protection and Measurements (NCRP)**
  - **National Defense University radiological event studies**
  - **National Response Framework**
  - **9/11 Commission Recommendations**
  - **TOPOFF 4**

Findings (cont.)

- National Defense University radiological study results
- Time is of the Essence
- They'll Look to the Feds
- Identify the Experts
- Deal the Private Sector In
- Psychological Impacts will Rival Physical Damage
- Psychological effects of events (including radiological events)
- Goainia, Brazil radiological accident, September 1987
- National Council on Radiation Protection and Measures
- NCRP Report No. 138, "Management of Terrorist Events Involving Radioactive Material," October 2001 addresses
- NCRP Commentary No. 19, "Key Elements of Preparing Emergency Responders for Nuclear and Radiological Terrorism," April 2006

Findings (cont.)

- **NCRP Commentary No. 19, "Key Elements of Preparing Emergency Responders for Nuclear and Radiological Terrorism," April 2006**
- **National Response Framework**
- **Issued by DHS for comment, September 10, 2007; 30-day comment period**
- **Objectives**
- **Radiological Annexes**
  - **Title V, Section 501, of the 9/11 Commission Act of 2007 - Strengthening the Security of Cargo Containers**
- **TOPOFF 4; TOPOFF 3 results not broadly disseminated**
- **Surveillance and Response**
- **Communications**

Nuclear Sector

- **Nuclear Sector Coordinating Council (NSCC)**
- **Nuclear Sector possesses inherent strengths against RDD or other potential threats posed by ionizing radiation.**
- **The nation could potentially:**
  - Develop and deploy training modules for all first responders by adapting existing industry training programs.
  - Explore Memorandums of Understanding for private-sector expert resource sharing during an RDD emergency—private-sector expertise is resident in most US states.
  - Leverage industry knowledge and experience in developing a credible communications strategy and assistance in tailoring messages for public release.

Nuclear Sector (cont.)

- **Substantial work done to analyze radiological threats, including RDD threats, considering both prevention and response.**
- **Regulatory oversight in all critical elements of the business.**
- **Deployable, trained, organized Emergency Response Infrastructure.**

Recommendations

- **Planning, preparedness, and response:**
  - Complete the prioritization of comprehensive, national risk assessment (e.g., RAMCAP, NIPP, etc.) that prioritizes radiological threats and vulnerabilities within context of others (e.g., chemical, biological, etc.).
  - Define roles and responsibilities for agencies that impact the transportation of, and accountability for, radiological materials.
  - Improve knowledge around specific scenarios, impact, and likelihood of events.
  - Improve accessibility to planning and response material.
  - Clearly define response roles, responsibilities, and communication protocols. Include as part of response exercises.
  - Improve planning, preparedness, and response capabilities across first responders.

Recommendations (cont.)

- **Surveillance and detection; tools and technologies:**
  - Improve information collection, analysis, and reporting mechanisms that support radiological event detection; define S&T roadmap on same.
  - Continue to fund collaborative, public-private efforts to develop more advanced detection solutions:
  - Accelerate deployment of tools/technologies under development; identify commercialization mechanisms making solutions more broadly available to public and private sector stakeholders.

Recommendations (cont.)

- **Communications:**
  - Continue to make progress with NIMS/NRF re-write:
  - Continue to make strategic improvements, including implementation of WARN Act and Safecom.
  - Improve tactical event communications capabilities, specifically around first responder, private sector, and fire/EMS/law enforcement resources.

Recommendations (cont.)

NDU Radiological Study Suggested:

- Early identification of impacts on key infrastructure.
- Understanding the government's capacity for response.
- Knowing who is in charge of the response.
- Receiving timely guidance on how to respond.
- Rapid delineation of radiation hazard zones.
- We found a great deal of information available on nuclear effects and response.
- Information is not yet adequately adapted for contemporary responders' needs.

Questions?

ATTACHMENT B

The Insider Threat to Critical Infrastructures

The Insider Threat to Critical Infrastructures

Thomas Noonan
General Manager
IBM Internet Security Systems

Edmund Archuleta
General Manager
El Paso Water Utilities

Overview

- **Objective**
- **Report Findings Highlights:**
  - **Defining the Insider Threat**
  - **Scope: Psychology and the Disgruntled Insider; Variation on Maturity and Awareness**
  - **Dynamics: Technology and Globalization**
  - **Obstacles to Addressing the Insider Threat**
  - **Developing Recommendations**
- **Next Steps**
- **Questions**

Objective

- **First Phase focused on defining the insider threat to critical infrastructures, including dynamics involved, obstacles to mitigation, and the effect of globalization.**
- **The second phase of the study will focus on legal, procedural, and policy barriers for private sector infrastructure operator employee screening efforts.**
- **Completion of the study may produce potential recommendations for improving operators' ability to address the insider threat to critical infrastructures, and seek to provide guidance on a clear legal environment for operators in dealing with potentially hostile insiders.**

Objective

- **First Phase focused on defining the insider threat to critical infrastructures, including dynamics involved, obstacles to mitigation, and the effect of globalization.**
- **The second phase of the study will focus on legal, procedural, and policy barriers for private sector infrastructure operator employee screening efforts.**
- **Completion of the study may produce potential recommendations for improving operators' ability to address the insider threat to critical infrastructures, and seek to provide guidance on a clear legal environment for operators in dealing with potentially hostile insiders.**

Insider Threat: Scope

- **Risk Management approach to protection: based on informed understanding of threat, vulnerability, and consequence**
  - **Identify and prioritize risks based on identification of critical assets**
- **Understanding threats**
  - **Actors and motivations**
  - **Importance of psychology and the "disgruntled" insider**
  - **Emerging Economic Espionage threat**
- **Variation on maturity and awareness of the insider threat**

Scope: Importance of Psychology and the "Disgruntled" Insider

- **The psychology of the "disgruntled" insider plays a role in understanding almost all insider threat cases**
  - **CERT/CC-US Secret Service study found commonalities between U.S. espionage cases and known cases of "disgruntled" insiders committing acts of IT sabotage**
  - **The Working Group is investigating links between disgruntled insider psychology and workplace violence cases**
  - **Needs more research**
- **The vast majority of disgruntled employees are not potential insider threats**
- **Common characteristics and common path to betrayal**
  - **Not a profile – a critical pathway**

Scope: Variation on Maturity and Awareness of Insider Threats

- **Awareness of the insider threat varies greatly among the critical infrastructure sectors**
- **Need baseline, common understanding of the risks for owner-operators**
  - **Misperception of risk can result in complacency and denial**
  - **Aware, but do not fully understand the risks and potential consequences**
- **To get CI owner-operators to actively manage insider risks:**
  - **Need common, clear understanding of the threat**
  - **Achievable, cost effective mitigation goals**
- **Need improved information on what is happening with insider incidents**
  - **Improved information sharing for better data and research – business intelligence level information**
  - **Effective communication of government threat information to owner-operators**

Dynamics of the Insider Threat

- **Technology and globalization risks are intertwined**
- **Industry is immature at detecting insiders**
- **Technology risks for companies are growing at a rapidly escalating rate – faster than the solutions**
- **Existing insider threat tools are expensive to deploy**
- **Significant, escalating technology threats:**
  - **Proliferation of small, mobile computing devices and constant network access are eroding traditional workplace boundaries**
  - **Threat tools are increasingly commonly accessible and easy to use, reaching greater group of potential insiders**

Globalization

- **Globalization affects different sectors in different ways and to different degrees**
- **Emerging globalization risks include:**
  - **Expanding the group of trusted insiders within a company to new populations – less verifiable, different cultural norms**
  - **Emerging global supply chain vulnerabilities**
- **Multinational corporations face legal obstacles**
  - **Legal deterrence for insider betrayal, Intellectual Property and patent protections, and enforcement of laws all can vary significantly**

Obstacles to Addressing the Insider Threat

- **Information Sharing on insider threats**
  - No reliable threat intelligence
  - No trusted entity for collection and protection
  - Little incentive to share information on insider incidents
- **Education and Awareness**
  - Need baseline understanding of insider threats
  - Need effective mitigation programs
  - Key to needed cultural change
- **Background Investigations**
  - Not universally accepted, no standard or common method
  - Periodic reinvestigation or monitoring for critical positions
- **Technology**
  - Threat tools growing faster than the solutions
  - Need more deployable, adaptable solutions
- **Cultural and Organizational obstacles**
  - Collaboration needed between IT, HR, Security, and asset owners to address insider threats
  - Culture and institutional momentum can hinder mitigation

Developing Recommendations

Plan to develop specific, actionable recommendations to address identified obstacles:

- **Information Sharing**
  - **Need government intelligence agencies to share relevant strategic level information on insider threats**
  - **Sectors need to establish a trusted process and mechanism to share incident information**
  - **Need an insider threat clearinghouse/resource for owner/operators seeking to assess and mitigate their insider risks**
- **Education and Awareness Framework**
  - **Executive and workforce education and awareness of insider threats**
  - **Senior Management implementation for affecting cultural change**
- **Background Investigations**
  - **Exploring during Phase II study**
  - **Examining the challenges facing infrastructure operators in developing risk-focused background investigation programs**
- **Technology**
  - **Investigating needed technology solutions**
  - **Has potential role in mitigating insider risks**
- **Cultural and Organizational Obstacles**
  - **Under Investigation**

Next Steps

- Begin*Phase II* research
- Working Group to finalize*Phase I* Report
- Research and develop specific, actionable recommendations for identified obstacles
- Write*Phase II* Report
- Publish Final Report at January 2008 meeting

Questions?