NATIONAL INFRASTRUCTURE ADVISORY COUNCIL (NIAC)

MEETING AGENDA

Tuesday, July 10, 2007
1:30 – 4:30 p.m. EDT
National Press Club
529 14th Street NW
Washington, D.C. 20045

I.	**OPENING OF MEETING**	*Gail A. Kaufman,* Designated Federal Officer (DFO), NIAC, Department of Homeland Security (DHS)
II.	**ROLL CALL OF MEMBERS**	*Gail A. Kaufman*
III.	**OPENING REMARKS AND INTRODUCTIONS**	NIAC Chairman *Erle A. Nye,* Chairman *Emeritus,* TXU Corp. *Robert B. Stephan*, Assistant Secretary for Infrastructure Protection, DHS *Thomas P. Bossert*, Acting Senior Director for Preparedness Policy, Homeland Security Council (HSC) *Neill Sciarrone*, Director of Protection and Information Sharing Policy, HSC
IV.	**APPROVAL OF APRIL MINUTES**	NIAC Chairman *Erle A. Nye*
V.	**PRIORITIZATION OF CRITICAL INFRASTRUCTURE FOR A PANDEMIC OUTBREAK RECOMMENDATIONS UPDATE**	*Rear Admiral W. Craig Vanderwagen, MD*, Assistant Secretary for Preparedness and Response, Health and Human Services (HHS)
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

B. THE INSIDER THREAT TO CRITICAL INFRASTRUCTURES	*Edmund G. Archuleta*, President and CEO, El Paso Water Utilities, NIAC Member; and *Thomas E. Noonan*, General Manager, IBM Internet Security Systems, NIAC Member
VII. NEW BUSINESS	NIAC Chairman *Erle A. Nye*, NIAC Members
VIII. CLOSING REMARKS	*Robert B. Stephan*, Assistant Secretary for Infrastructure Protection, DHS
XI. ADJOURNMENT	NIAC Chairman *Erle A. Nye*

MINUTES

NIAC MEMBERS PRESENT IN WASHINGTON:

Mr. Erle A. Nye; Mr. Edmund G. Archuleta; Mr. Alfred R. Berkeley, III; Chief Rebecca F. Denlinger; Lt. Gen. (ret.) Albert J. Edmonds; Chief (ret.) Gilbert G. Gallegos; Ms. Margaret E. Grayson; Ms. Martha H. Marsh; Mr. James B. Nicholson; Mr. Gregory Peters; Mr. Bruce Rohde; and Dr. Linwood H. Rose.

NIAC MEMBERS ATTENDING VIA CONFERENCE CALL:

Mr. George H. Conrades.

MEMBERS ABSENT:

Dr. Craig R. Barrett; Commissioner Raymond W. Kelly; Mr. Thomas E. Noonan; Hon. Tim Pawlenty; and Mr. John W. Thompson.

SUBSTANTIVE POINTS OF CONTACT PRESENT IN WASHINGTON:

Mr. Peter Allor (for Mr. Thomas E. Noonan); Ms. Ellen A. Black (for Chief Rebecca F. Denlinger); Mr. Scott Blanchette (for Ms. Martha H. Marsh); Ms. Joan S. Gehrke (for Mr. James B. Nicholson); Dr. Ronald R. Luman (For Mr. Alfred R. Berkeley, III); Ms. Deborah Miller (for Ms. Margaret E. Grayson); Mr. Bill Muston (for Mr. Erle A. Nye); and Ms. Diane VanDe Hei (for Mr. Edmund G. Archuleta).

SUBSTANTIVE POINTS OF CONTACT ATTENDING VIA CONFERENCE CALL:

Lt. Paul Mauro (for Commissioner Raymond W. Kelly); Mr. Jason Rohloff (for Gov. Tim Pawlenty); and Mr. David Rose (for Dr. Craig R. Barrett).

OTHER DIGNITARIES PRESENT:

Col. Robert B. Stephan, Assistant Secretary, Office of Infrastructure Protection, DHS; Mr. Thomas P. Bossert, Acting Senior Director for Preparedness Policy, HSC; Ms. Neill Sciarrone, Director, Protection and Information Sharing Policy, HSC; Rear Admiral (RADM) W. Craig Vanderwagen, MD, Assistant Secretary for Preparedness and Response, HHS; and Ms. Gail A. Kaufman, DFO, NIAC, DHS.

I. OPENING OF MEETING

Ms. Gail A. Kaufman introduced herself as the DFO for the NIAC. Next, she welcomed Mr. Thomas P. Bossert, Acting Senior Director for Preparedness Policy, HSC; Ms. Neill Sciarrone, Director, Protection and Information Sharing Policy, HSC; Col. Robert B. Stephan, Assistant Secretary for Infrastructure Protection, DHS; RADM W. Craig Vanderwagen, MD, Assistant Secretary for Preparedness and Response, HHS; Mr. Erle A. Nye, NIAC Chairman; and all 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. Kaufman called to order the NIAC's 20th meeting and the third meeting of 2007.

II. ROLL CALL

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

III. OPENING REMARKS AND INTRODUCTIONS

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

Robert Stephan, Assistant Secretary for Infrastructure Protection, DHS

Thomas P. Bossert, Acting Senior Director for Preparedness Policy, HSC

Neill Sciarrone, Director of Protection and Information Sharing Policy, HSC

Chairman Nye welcomed everyone to the meeting and noted the excellent attendance. He reminded everyone of the meeting's public nature, stressing the importance of not discussing confidential information. Chairman Nye thanked Ms. Kaufman on behalf of the NIAC for her work and announced she accepted a position with the Office of Strategic Plans at DHS headquarters. He added the Council was pleased she found such an opportunity and will miss her.

Chairman Nye continued by saying Secretary Chertoff and Ms. Frances Fragos Townsend, Assistant to the President for Homeland Security and Counterterrorism (APHS/CT), regretfully could not attend the meeting. He thanked Assistant Secretary Stephan for attending and looked forward to any feedback or guidance the Assistant Secretary might offer. Chairman Nye also thanked Mr. Bossert, Ms. Sciarrone, and RADM Vanderwagen for meeting with the Council. He then asked the White House representatives for comments.

Mr. Bossert thanked the Chairman for the opportunity to attend and said the NIAC's work represented an impressive achievement.

Ms. Sciarrone also thanked the Chairman for the invitation and lauded the NIAC for their dedication. She added the White House would continue to search for new Council members as well as identify a new Vice Chairman for the Council.

Chairman Nye asked Assistant Secretary Stephan if he had any comments, and the Assistant Secretary deferred his comments for later in the meeting.

IV. APPROVAL OF APRIL 10, 2007 MINUTES

NIAC Chairman, *Erle A. Nye*, Presiding

Chairman Nye moved to the review and approval of the April 10, 2007 NIAC Meeting Minutes. He asked the Council for amendments or additions to the minutes. The members voiced no corrections or comments. Chief (ret.) Gilbert G. Gallegos moved to approve the minutes, and Lt. Gen. Albert Edmonds seconded the motion. The Council unanimously approved the motion.

V. PRIORITIZATION OF CRITICAL INFRASTRUCTURE FOR A PANDEMIC OUTBREAK RECOMMENDATIONS UPDATE

Rear Admiral W. Craig Vanderwagen, MD, Assistant Secretary for Preparedness and Response, HHS

Chairman Nye asserted both DHS and HHS commissioned the Council to study the prioritization of activities in the event of an influenza pandemic. In February 2007, the Council produced the *Prioritization of Critical Infrastructure for a Pandemic Outbreak in the United States Report and Recommendations* in an effort co-chaired by Council members Ms. Martha H. Marsh, Chief Rebecca F. Denlinger, and Mr. Bruce Rohde.

Chairman Nye introduced RADM Vanderwagen to update the Council on the implementation of its pandemic recommendations. Chairman Nye said the NIAC always appreciates RADM Vanderwagen's remarks and thanked him for providing the Council with valuable feedback.

RADM Vanderwagen thanked Chairman Nye and expressed his appreciation for the Council's meaningful and detailed assessment of the required critical infrastructure workforce especially at risk during a pandemic. The NIAC provided pandemic planners with descriptions of the 17 critical infrastructure sectors' essential functions. This supplied the Public Health and Healthcare sector with insight into the needs of other sectors and into the requirements needed to sustain the nation's economy during large-scale national emergencies. These insights remain applicable beyond a pandemic incident and retain value for biological incidents or other widespread events requiring medicine prioritization.

According to RADM Vanderwagen, the NIAC study's outcome provided HHS with a baseline from which to explore and refine essential workforce numbers within each sector as HHS prioritizes and develops plans. The Center for Disease Control (CDC) used the report and the sector workforce estimates from the *Prioritization of Critical Infrastructure for a Pandemic Outbreak in the United States Report and Recommendations* to yield four prioritization categories with five vaccination tiers in each category based on a pandemic severity index. In order to help the public conceptualize pandemic severity, HHS adopted a rating system similar to the one used by the National Hurricane Center (NHC). NHC uses a one-to-five ascending severity ratings system to gauge a hurricane's potential for property damage and loss of life. As applied to influenza, a Category 1 influenza outbreak would represent a stronger-than-usual seasonal flu while a Category 5 would signify an event parallel to or even exceeding the 1918 Spanish Flu. HHS also quantified and calculated lethality for the index. With this new system in place, the government can discuss a pandemic's expected impact on a community.

In addition to the influenza severity rating system, HHS uses a tiered system to structure and test public health models. Tier 1 consists of those people in the most critical occupations—the general population resides at the far end of the scale. HHS converted the numbers provided in the NIAC report into a critical occupation prioritization plan for a Category 5 event with limited vaccine.

The NIAC's Report and Recommendations help HHS guide states' vaccination and antiviral distribution plans. While DHS and HHS did not specifically ask the NIAC to examine antivirals,

Roche's standup of expanded industrial capability allows enough antiviral production to consider prophylaxis. As HHS begins to examine prophylaxis, any guidance HHS could provide business and industry in distributing antivirals to their employees would be beneficial. The NIAC's report provides a framework for HHS to use in helping businesses consider stockpiling prophylaxis antivirals. Based on the NIAC report numbers, HHS conducted an analysis of tiering that provided insight towards developing a public health modeling of rationing limited assets during a health emergency; HHS may even use the report in other settings and asset assessments.

The Rear Admiral hoped within the next three months HHS would not need to discuss rationing vaccines. Recent developments in adjuvant technology allow the combination with vaccines to increase immune system response twenty-fold, and an increase of this magnitude means manufacturers can reduce the vaccine's concentration twenty-fold and still generate the same immune system response in the vaccinated individual. HHS is currently looking at the use of adjuvant with other H5N1 vaccines to confirm its safety and effectiveness. If these trials prove to be successful, the government might be able vaccinate everyone in the country without prioritization.

RADM Vanderwagen asserted HHS might return to the Council with a specific request for assistance regarding the shared responsibility of gap analysis for protective gear like masks and ventilators. HHS could utilize the NIAC's considerable insight and expertise in its tactical decision-making. Many pandemic-specific issues lay ahead potentially meriting discussion between NIAC and HHS. He concluded his remarks by thanking Chairman Nye and the Council again.

Chairman Nye thanked RADM Vanderwagen for attending and providing feedback. The Council takes pride in hearing the impact of its work. He thanked Ms. Marsh, Chief Denlinger, and Mr. Rohde for their leadership and thanked everyone else who worked on the *Prioritization of Critical Infrastructure for a Pandemic Outbreak in the United States Report and Recommendations*. Chairman Nye again thanked RADM Vanderwagen and turned to Working Group preliminary findings.

VI. WORKING GROUP PRELIMINARY FINDINGS

NIAC Chairman, *Erle A. Nye*
Presiding

Chairman Nye moved on to introduce the two Working Groups presenting their preliminary findings:

- Chemical, Biological and Radiological (CBR) Threats and the Impacts to the Critical Infrastructure Workforce and
- The Insider Threat to Critical Infrastructures.

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 stated the Chemical, Biological and Radiological (CBR) Events and the Critical Infrastructure Workforce Working Group addressed biological threats before Secretaries Chertoff and Leavitt tasked the Group with the *Prioritization of Critical Infrastructure for a Pandemic Outbreak in the United States* study. The Working Group, currently chaired by Ms. Martha Marsh, Chief Rebecca Denlinger, and Mr. Bruce Rohde, is presently working on the chemical portion of the study and intends to report its preliminary findings during the meeting. Chairman Nye hoped the Working Group would begin working on the radiological issue before the next NIAC meeting.

Ms. Marsh greeted Assistant Secretary Stephan, RADM Vanderwagen, the NIAC members, and everyone present. She stated Mr. Scott Blanchette would start the briefing and she would follow with recommendations.

Mr. Blanchette thanked Chairman Nye and RADM Vanderwagen for his feedback on the pandemic study. He said it represented an intensive effort from the Council and was pleased to hear it was valuable and well received.

Mr. Blanchette stated the CBR Study Group wanted to present their progress specifically recapping its objectives, timeline, and mission statement. The Study Group wanted to provide its preliminary findings to precede the Working Group's final recommendations at the October NIAC meeting.

Since its inception in January 2007, the Study Group focused on chemical threats and vulnerabilities, as well as identifying findings to improve critical infrastructures' ability to identify and respond to such an event. Within the scope of this assignment, the Study Group worked to identify elements of the critical infrastructure crucial to responding to a chemical event. They identified studies quantifying the statistical probability and potential impact of a chemical incident. The Study Group also further studied how critical infrastructure entities develop and implement response capabilities. Finally, the Study Group identified gaps in preparedness and response capabilities.

He added the Study Group research structure focused on six key questions:

1. Do organizations have employee awareness, preparedness, and response training programs?
2. Is there a market incentive to invest in chemical preparedness and response programs?
3. Is sufficient communication infrastructure in place to respond to a chemical event?

4. What tools and technologies currently support chemical response capability?
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?

The group designed these questions in an attempt to understand the many aspects of chemical events threats, vulnerabilities, response plans and programs, supporting communications infrastructure, as well as the economics involved in preparing for a possible chemical event.

Over the past few months, the Study Group received numerous valuable presentations and benefited from extensive support across both public and private sectors. He noted DHS certainly met the Study Group's April request for additional support.

The Study Group identified many studies designed to quantify the threat and vulnerability picture. These studies came from many agencies within government, academia, and the private sector. Due to the sheer number and breadth of these reports, the Study Group opted to present a few high-profile assessments. In one example, DHS identified 15,000 chemical facilities, when affected by an incident, could adversely affect local populations. The same study identified more than 3,400 facilities threatening over 1,000 people in the case of an event.

These facilities were further tiered by the effect produced by an incident at each facility and the ability of the incident to impact the population. A Tier 1 facility affects more than 1.4 million people; a Tier 4 facility affects between 1,000 and 49,999. There is a good deal of interpretation for general cause and effect data due to multiple reasons. For example, in all cases, the agent's effect depends on:

- Purity of the chemical;
- Concentration in the air;
- Wind and weather conditions at the time of release;
- Length of exposure;
- Dispersion characteristics (e.g., water or liquid-based, airborne, triggered by compounds, etc.);
- Ability to obtain or assemble significant source volumes or concentrations; and
- Ability to make it airborne (e.g., a heavy liquid not volatile at room temperatures).

Mr. Blanchette described the Aum Shinrikyo cult that experienced problems producing and weaponizing Sarin gas as a mass casualty weapon as one example of the difficulty in gaining consensus on threat and vulnerability data. They spent an estimated $30 million on chemical weapons research and killed 19 people in their high-profile 1995 subway attack. In that event, a wide interpretation on "investment versus return" exists. In contrast, a number of studies suggest this was a poorly executed attack and a better-planned attack could produce many more casualties and more damage at a lower cost.

Through the course of its study, the Study Group identified many examples of progress improving the nation's ability to identify or detect chemical events. DHS and the Federal Emergency Management Agency (FEMA), HHS and CDC, numerous state-level activities, and a host of public-private partnerships are a few examples identified as part of the Study Group's surveillance and detection inquiries.

Mr. Blanchette said the Study Group sought to comment on the Chemical Comprehensive Review and the work to better understand the chemical event problem statement as a complete body of work. Specifically, CCR focused on the following areas:

- Threat analysis;
- Facility characterization;
- Assault planning;
- Explosive ordinance disposal;
- Law enforcement resources;
- Emergency response resources; and
- Maritime and transportation resources.

He added the Study Group wanted to brief the NIAC on the tremendous progress made in joint, collaborative, or otherwise cross-functional efforts to improve chemical event preparedness and response capabilities. They found examples of Federally sponsored planning and response coordination efforts, such as the Community Hazards Emergency Response-Capability (CHEMTREC) Assurance Process.

CHEMTREC represents an industry-sponsored program supporting first responders who support chemical or other hazardous material event response. The Study Group identified many examples of mutual aid organizations and fusion centers. Charleston, South Carolina's *Project Seahawk* exemplifies an integrated Federal, State, local, and private sector emergency response command center. In its research, the Study Group also identified a suite of tools designed to improve assessment, planning, incident management, and resource coordination capabilities. The Study Group also found both public- and private-sector preparedness varies according to a number of factors, including the nature of the sector, geography, or maturity of emergency response capabilities.

Mr. Blanchette stated the Study Group would not spend much time addressing communications findings except to describe chemical-specific communications progress. He commented the vast majority of communications advances identified derived from broader, more comprehensive general emergency event communications investments. This reflects the advantage one would expect to see from investments in broadly usable communication technologies in multiple scenarios.

DHS recently enacted anti-terrorism standards that went into effect June 8, 2007. There were four primary objectives of this standard:

1. Provide uniform national chemical facility security standards;
2. Provide reasonable preemption if state laws conflict;
3. Create protected Chemical-Terrorism Vulnerability Information (CVI) and ensure information dissemination to state, local, and other first responders;
4. Ensure recognition of standards already achieved

To implement these objectives, DHS outlined the following processes:

1. 40,000 facilities were tasked to complete a consequence-screening questionnaire.
2. DHS assigned a risk rating for each facility.
3. High-risk facilities were tasked to complete a more comprehensive vulnerability assessment.
4. At-risk facilities were tasked with developing a risk remediation plan and implementation timeline.
5. This standard also includes elements of audit and enforcement actions.

He noted current projections suggest 5,000 to 8,000 at risk facilities with 300 in the top two tiers.

Mr. Blanchette stated the Study Group's studies suggested preparedness directly correlated to an organization's size. Large organizations tended to possess more and better examples of event preparedness and response capabilities. The opposite is true for smaller organizations. The Chemical Sector presented many instances of self-organizing and self-funded initiatives to improve their collective risk assessment and emergency response capabilities. Perhaps most remarkable was the percentage of organizations complying with and adopting the industry's security standards and programs.

Mr. Blanchette pointed out the majority of the group's recommendations focus on five key areas:

1. Planning preparedness and response;
2. Surveillance and detection;
3. Communications;
4. Regulations; and
5. Policy, specifically international policy.

Chief Denlinger continued by pointing out the Working Group's first set of proposed recommendations focus on improving planning, preparedness, and response capabilities. The Working Group identified many positive models of solid progress to improve planning and response capabilities. They suggest a comprehensive, national risk assessment to assess and prioritize chemical threats and vulnerabilities within the context of others threats (e.g., biological and nuclear incidents). The Working Group found some degree of competing or overlapping jurisdictions existing across agencies tasked with end-to-end chemical event assessment,

planning, preparedness, and response. Perhaps more accurately, a less than clear understanding exists among stakeholders on this issue. They recommended more clearly defined roles and responsibilities for agencies overseeing the transportation of, and accountability for, chemicals, including Customs and Border Protection (CBP), Transportation Security Administration (TSA), Department of Transportation (DOT), and the U.S. Coast Guard (USCG). Furthermore, public-sector incident response roles and responsibilities require guidance on all levels on how these entities should work with the private sector.

Over the course of the study, the Working Group recognized the mass of valuable information shared through numerous venues, including efforts to enable the Sector Specific Agencies (SSAs) to serve as information conduits to the private sector through bi-weekly calls. The Working Group would suggest continued efforts to improve knowledge around specific scenarios, the scenarios' impact, and the likelihood of these events materializing. The Working Group would also recommend improved access to critical planning data potentially affecting organizational response plans or programs. If possible, it would be beneficial for key private-sector stakeholders with access to Chemical-Terrorism Vulnerability Information (CVI) information to be involved.

Chief Denlinger stated the first responder level most clearly lacked response capabilities. The Working Group found limited mechanisms in place to improve accessibility and economic viability of necessary equipment. Additionally, first responders, especially law enforcement and local fire/EMS, possess varied readiness levels affecting their response to potential chemical events.

The Working Group would encourage continued efforts in surveillance and detection, as well as in communications capabilities. It identified a number of technologies intended to improve surveillance and detection. Due to limited access to source data, timelines for implementation of those technologies remain undefined. At a tactical level, the Working Group continued to find examples of improvements in communications interoperability, but the number of instances of poor interoperability suggested a need for continued focus and effort on this front.

Chief Denlinger asserted the Working Group generated multiple valuable recommendations during their study. The core of these being two fundamental thoughts, the government must:

1. Develop and implement more efficient risk- and threat-based regulations to reduce the duplicative existing requirements across multiple agencies
2. Determine a means to improve the consistency of chemical standards across borders.

Chief Denlinger told the attendees the SSA should act as the lead for the reduction of duplication and the development of risk management processes and requirements. The final solution should accommodate other agency missions, goals, and objectives, but there should be a single, accountable entity driving this process to conclusion. The current environment, characterized largely by competing or overlapping standards and regulations, is neither efficient nor productive.

Encouraging the global ratification and implementation of treaty requirements such as the Chemical Weapons Convention (CWC) requires a great deal of international work. CWC's sanction, along with other similar mandates, would level the playing field for the chemical trade and limit chemical weapon diversion or proliferation. This effort would seek to drive global adoption of improved, risk-based site security measures, address border control measures, and ensure enforcement consistency. To be successful, it would need to provide incentives and support for global adoption of reasonable safety and security practices such as those implemented by the International Coalition of Chemical Associations for over 70 percent of chemical industry operations in 52 countries around the globe.

Chief Denlinger said improved assessment of the risks of border controls and containment on chemical security remains important. Government and industry must correlate border controls to other domestic chemical security measures to ensure consistency.

Chief Denlinger thanked Chairman Nye for the opportunity to provide her update. She concluded her remarks by saying the Working Group will provide its Final Report and Recommendations at the October 9, 2007 NIAC meeting. She welcomed any questions or comments.

Mr. Alfred R. Berkeley, III asked if the extensive risk analysis on chemical plants justifies revisiting the Council's *Common Vulnerability Scoring System (CVSS) Report and Recommendations* released October 12, 2004 to include any new information. With thousands of plants responding and scoring in a hypothetical model, this information could be very useful.

Chairman Nye told the attendees the CVSS topic would be included in future NIAC initiative discussions. He then asked Assistant Secretary Stephan for any comments.

Assistant Secretary Stephan thanked the Working Group for its preliminary findings and ensured the meeting attendees that his team continues working to implement the chemical facility regulatory framework launched on June 8, 2007. DHS will take all of the Council's recommendations into consideration as it continues evolving its programs in concert with private-sector owners and operators. It will also extend the recommendations to its State and local counterparts who play an integral role in the planning process to develop plans addressing gaps identified during the risk assessment process. DHS will then implement joint solutions linking the inside- and outside–the-fence security. Assistant Secretary Stephan stated this study will be timely to help meet these goals and asked if DHS could extract recommendations from the Working Group's findings before the Council finalized the report. The Assistant Secretary reiterated a suggestion made by RADM Vanderwagen that the Council consider adding a recommendation inside its study framework suggesting improving medical countermeasures in respect to the chemical threat vector.

Chairman Nye thanked the Assistant Secretary for his suggestion and asked Working Group member Mr. James Nicholson if he would like to add any additional remarks stemming from his expertise in the chemical industry.

Mr. Nicholson stated DHS appeared on the right track with the Department's June 8 implementation. He hoped DHS received sufficient cooperation from the industry and offered his assistance if the Department needed more. He added the CBR task represented a difficult undertaking as it hinges on a defensive rather than offensive stance. He thought the industry remained generally pleased with the work accomplished thus far.

Chairman Nye thanked Mr. Nicholson and asked if there were any other comments or questions. He assumed the work on the chemical study would continue while the radiological review would begin simultaneously. He anticipated potential approval in the fall.

Mr. Blanchette confirmed Chairman Nye's timeline aligned with the Study Group's goals.

Chief Denlinger added a challenge of this study continues to be working in an area where public and private sectors converge.

Chairman Nye thanked the Working Group for its work and progress.

B. THE INSIDER THREAT TO CRITICAL INFRASTRUCTURES — *Edmund G. Archuleta*, President and CEO, 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.

Mr. Archuleta greeted Chairman Nye, Assistant Secretary Stephan, Thomas Bossert, Neill Sciarrone, Gail Kaufman, and his fellow Council members. He thanked the members of the Working and Study Groups. Initially, the Working Group met with the White House to ensure it fully understood the study's scope. The first task involves defining the problem and then initial analysis. The Working Group holds weekly meetings to discuss the insider threat issues. He said the Working Group wanted to present an executive summary as well as some preliminary findings. He then introduced Mr. Peter Allor to present the briefing.

Mr. Allor thanked Mr. Archuleta and stated the White House vetted the Insider Threat Working Group's scope. The Study Group continues working to maintain the objectives presented at the April NIAC meeting. Started in April 2007, Phase I will conclude in October 2007. It includes:

- Defining the physical and cyber insider threat, including potential consequences, economic or otherwise;
- Analyzing the dynamics and scope of the insider threat including critical infrastructure vulnerabilities;
- Analyzing the potential impact of globalization on the critical infrastructure marketplace; as well as
- Identifying/defining the obstacles to addressing the insider threat.

The objectives in Phase II, derived from Secretary Chertoff's letter, include:

- Identifying issues, potential problems, and consequences associated with screening employees;
- Identifying legal, policy, and procedural barriers aspects of the issue, as well as any potential obstacles, from the perspective of the owners and operators; and
- Identifying policy recommendations on potential remedies for addressing the insider threat (up to and including potential legislation).

The Study Group divided the study into foundational items and into more in-depth questions about what would work best for critical infrastructures. The Study Group held its first face-to-face meeting, which included a brief by Computer Emergency Response Team Coordination Center (CERT/CC) on a study on which they had worked with the United States Secret Service (USSS). The meeting also featured representatives from the Federal Bureau of Investigation (FBI) to provide their perspective to the study. The Study Group compiled a significant amount of initial materials and information from the public sector to build a framework as they reach out to the private sector for their input.

The Study Group spent more time than expected to define the insider threat, but this extra time allowed it to reexamine the definition to ensure its integrity. The definition identifies an insider threat 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."*

Mr. Allor said the focus of the group remains on critical infrastructure to ensure the study applies to each of the 17 sectors. The Study Group found it must be careful not to dilute the study by trying to encompass all threats.

The Study Group expects the scope analysis for the study will extend past the October 2007 period into Phase II for modification. It identified the following key issues regarding scope:

- Focus on critical infrastructure-level threats—threats affecting CI services delivery, the economic backbone, or public health/safety.
- There is significant variation among sectors on maturity and awareness of insider threats.
- Potential actors include disgruntled employees, economic espionage, and infiltration.

The dynamics and obstacles remain well intertwined. Mr. Allor pointed out the threat to critical infrastructure and the economic backbone is not only part of the definition, but a part of the dynamics as well, and thus the group is finding more interrelationship than originally anticipated. The Study Group identified the following key points regarding the dynamics of the insider threat:

- There is a lack of hard data for universal definition
- Globalization is escalating exposure and costs of these threats
- Technology and network risks are rapidly escalating
- Complacency and denial are key components

Mr. Allor said the Study Group found many differences between sectors, most of which depend on sector maturity and awareness. The Study Group found the threats differ from previous expectations. While disgruntled employees causing asset loss represents a real concern, some sectors show greater concern for economic espionage and infiltrations. The Study Group also found it difficult to gather data on some of these topics due to maturity and sensitivity issues. While much information exists regarding cyber threats, there is a severe lack of data and analysis on physical threats. Certain dynamics also cause concern in technology's use and in the increasing use and interconnectivity of networks.

Mr. Allor also pointed points out one can see the link between the obstacles and issues raised in the scope and dynamics. The Study Group identified the following obstacles:

- Due to a lack of hard data, threat definition remains difficult;
- While education and awareness can be provided, cultural change remains more difficult and requires:
  - Investment in structured programs and risk management;
  - Corporate culture where trust does not run counter to prevention programs; and
  - Improved workforce communication and cooperation so targeted efforts can address insider threats
- Use of background checks varies among sectors and are not universally accepted; regulation is controversial; and
- Multiple legal environments complicate Insider Threat mitigation strategies, not only domestically, between Federal, State, local jurisdictions, but also and more significantly, for those companies operating in multinational environments, complicating cohesive or comprehensive policy efforts.

The Study Group opened its study by confronting the dearth of hard data on insider threats. It worked with several companies that discussed challenges in dealing with recent insider threat situations with potential as case studies. The Study Group also found educational awareness to be an inexpensive method for heightening the public's knowledge about these threats. Additionally, there seems to be reluctance from both management and employees to accept a continual background screening process. Finally, the legal environment has some complicated factors like dealing with problems across the international marketplace.

Mr. Allor then addressed the Study Group's concerns with globalization. Some factors the Study Group wanted to address with this issue include:

- Introducing enormous macroeconomic forces to the marketplace thus pushing large scale changes and introducing new threats for critical infrastructure operators
- Expanding IT networks and increasing risk
- Expanding the group of insiders thus creating populations that are less verifiable, and may be less reliable
- Varying legal environments among different countries complicate mitigation policies
- The global supply chain used by infrastructure operators is increasing potential for expanded insider threats or agents

The rush to globalization is incorporating a wider range of markets for companies, but it is also allowing new threats to surface. This is similar to a cyber network in that when one increases a network's size, the perimeter increases and weakens and the complexity increases and becomes a challenge. Larger companies may have begun to tackle these issues, but many smaller companies may not have identified this as a problem.

Mr. Allor wrapped up his report, stating that the Group should finish its Phase I tasks by the October 2007 NIAC meeting and will be prepared to offer those findings. He also expected the draft of that report to be published by January 2008. The Group is planning to begin its Phase II research in October 2007, but because of overlap, work on Phase II could begin as soon as September or late August. Mr. Allor said that he expected the Phase II research to be completed by January 2008 and could be reported by March 2008. The Study Group has a two-day workshop planned for July 2007 to include discussions with corporate security from different companies, as well as other public- and private-sector individuals who deal with both the cyber and physical aspects of the insider threat on a day-to-day basis. Mr. Allor expressed his gratitude to all the study group members for their commitment and service.

Chairman Nye thanked Mr. Allor and commented on the difficulty of this Working Group's task. He expressed hope the Study Group will produce some valuable recommendations that DHS can embrace. The Chairman noted the insider threat topic's recent media exposure and the timeliness of the NIAC's efforts on the subject He then offered all members of the Council an open invitation to join the Study Group. Mr. Nye asked for any further questions or comments. Receiving none, he then thanked the group for their work.

VII. REMARKS

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

Having heard presentations from the two current NIAC Working Groups, Chairman Nye asked for Assistant Secretary Stephan's comments. The Assistant Secretary offered the support of his staff to expedite the NIAC Working Groups' progress.

Assistant Secretary Stephan thanked Chairman Nye and said the reports were very thorough and informative. Over the last several months, DHS reached some very important milestones in the Critical Infrastructure Protection (CIP) mission; specifically regarding the NIAC's *Sector Partnership Model Implementation Report and Recommendations,* as well as the National Infrastructure Protection Plan (NIPP). DHS recently celebrated the first anniversary of the NIPP implementation and the framework embraced in the public-private sector partnership. Two months ago, Secretary Chertoff issued a set of 17 SSPs transcending the NIPP framework to tailor the risk analysis and management framework for each sector. These plans form a comprehensive base line connecting each sector to measure milestones and timelines.

Assistant Secretary Stephan continued, adding only a week before the NIAC meeting, DHS received the first sector annual report. These sector reports provide a complete examination of security from the perspective of each of the 17 sectors. They identify where sector security stands, the location of any remaining gaps, efforts necessary to collaborate in the future, and the timelines follow from the SSP. For the first time, DHS has a comprehensive set of security requirements analyzed from the public- and private-sector perspective.

He added he continued to push prioritized modeling simulation analysis pieces to the National Infrastructure Simulation and Analysis Center (NISAC) labs at Sandia and Los Alamos for analysis. In cooperation with Admiral Jay M. Cohen, Under Secretary for Science and Technology, Assistant Secretary Stephan and his staff worked to determine what solution might exist in the National Labs. The Assistant Secretary expressed his excitement to be able to present these enhancements across the sectors.

In June, DHS held a senior offsite meeting within OIP with stakeholders from the private sector as well as State and local governments who attended to offer feedback on DHS' performance. While they reached a joint agreement, some planning continues to require refinement, especially in the pandemic influenza piece.

He stated DHS is focusing on four objectives as this administration closes out:

1. SSP implementation—there is no need for a significant amount of new planning over the next eighteen months, but the goal to produce deliverables, achieve milestones, and meet timelines;
2. Risk Analysis;
3. Risk-informed grant process for 2008 using the Tier 1 and Tier 2 structure DHS finalized; and
4. Results of the annual data call process recently turned in by State Homeland Security Advisors

DHS continues examining pandemic influenza planning workshops and tabletop exercises across the 17 sectors. DHS also maintains working with the Partnership for Critical Infrastructure Security (PCIS) to ensure robust private sector engagement in the TOPOFF 4 exercise conducted in October 2007 involving radiological terrorism events in Portland, Oregon, Phoenix, Arizona,

as well as Guam. Assistant Secretary Stephan invited the NIAC members and their staffs to participate in the processes leading up to the October TOPOFF 4 event.

He pointed out DHS has been working with the SCCs to develop a training and awareness plan to further implement the NIPP and the SSPs across the country. DHS made its first comprehensive online education materials suite and training courses available through the NIPP section of the DHS website (www.dhs.gov/NIPP). DHS just launched the first certified training course for public- and private-sector infrastructure protection professionals in conjunction with the Federal Law Enforcement Training Center in Georgia.

Assistant Secretary Stephan stated over the next 18 months, DHS would focus on State and local government capabilities based on the NIPP framework. He added he met with the Homeland Security advisor and the Pennsylvania Governor's cabinet of along with three dozen private-sector companies the week prior to the NIAC meeting. Pennsylvania adopted the NIPP as its central approach to infrastructure protection, uses a Pennsylvania Infrastructure Protection Plan (PIPP) with SCCs organized across the 17 sectors, and an information-sharing network.

Assistant Secretary Stephan stated DHS is implementing the chemical security regulatory framework. This must continue to be a collaborative partnership. DHS builds upon the relationships and experience it gained promoting a voluntary security environment with the Chemical Sector over the past four years. DHS intends to build upon this approach. DHS will be finalizing the Chemical Comprehensive Review program in late 2007. This will provide comprehensive State and local government as well as private-sector facility security plans to 394 of the top Environmental Protection Agency (EPA) Risk Management Program (RMP) database facilities. These plans place consideration into items such as potential human life consequences or toxic inhalation release consequences. DHS intends to install regulatory authority over a voluntary security landscape. The Department has thus far filled gaps in planning and capabilities in America's most at-risk jurisdictions through Federal grants. This process focuses on both internal and external measures using regulation as a tool to supplement voluntary efforts where appropriate. These efforts also ensure fine-tuned collaboration with facilities directly affected by regulations as well as with State and local law enforcement jurisdictions where these plants are located.

He continued, saying DHS now sought to continue honing its incident management framework established over the past several years to ensure the CIP component would withstand a natural or man-made disaster. DHS accomplished this in a comprehensive final draft of the National Response Plan (NRP) addressing infrastructure protection, security assessments, restoration and recovery, information sharing, and building a common operating picture. The Department remains engaged in a series of tabletop exercises with its private-sector counterparts to make sure it addresses the entire scope. DHS will use this plan for the 2007 hurricane season. The Assistant Secretary pointed out DHS now possesses a cadre of 78 protective security advisors (PSAs) in the major urban areas across the United States connected to the following agencies:

- FBI,
- Secret Service,

- FEMA regional directors,
- State and local law enforcement,
- Homeland Security Advisors, and the
- Private-sector owners and operators of the most critical facilities inside their areas of responsibility.

On a daily basis, the PSAs cement relationships across public and private sector boundary lines, build security and emergency response, and remain the first responders on a scene to address any potential problems. These advisors compliment the Federal response structure and know the people and necessary contacts to fulfill their mission.

DHS continues to work with DoD and the intelligence community to assess the situation in Iraq and Afghanistan in terms of terrorist techniques and procedures. Terrorists use these tactics against coalition forces as well as with other bombings and terrorist activities occurring in other countries targeting critical infrastructures and public facilities. DHS is exporting those lessons learned to the owners and operator community in the United States. The recent plots at John F. Kennedy International Airport as well as the London and Glasgow events highlight the importance of the infrastructure protection information sharing network and partnership the NIAC recommended. This partnership produces and distributes written intelligence and information products to private-sector owners and operators and state and local government counterparts. It also seeks comments on where DHS needs to go in terms of protective recommendations based upon those evolving threat scenarios.

DHS incorporated the recent lessons from those experiences into an interactive tripwire bombing prevention network accessible to state and local bomb prevention and bomb squad commanders nationwide as well as private-sector security officials. Because of all the successes, London invited the U.S. bomb prevention team to participate in their ongoing investigation. Assistant Secretary Stephan said he kept an eye on the UK situation as British authorities continue their investigation. DHS continues gleaning those lessons and tying them into the information sharing networks.

The Assistant Secretary lauded the NIAC for being at the forefront of this progress. He thanked Chairman Nye and the Council for their hard work.

Chairman Nye thanked Assistant Secretary Stephan for his continued interest in the Council and added the NIAC counts on his guidance and support.

VIII. NEW BUSINESS

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

Chairman Nye believed the Council should continue its work and not scale back its efforts despite the upcoming Presidential election. Though the next President may appoint different members, the new President would retain some members for their expertise and backgrounds. The NIAC produced 13 reports of great value and tremendous insight.

The NIAC must now address its next steps. The Council's initiatives often stem from White House direction. Similar leads also come from DHS and occasionally from the Council and its interaction with both the private sector and government. Chairman Nye announced the Council's need to prepare new initiatives for when the current Working Groups complete their studies. Chairman Nye asked his substantive point-of-contact, Mr. Bill Muston, to gauge the Council's interest in new topics. The Chairman added though the Council may be given direct guidance on what it should do, it should be prepared in case this does not happen. Chairman Nye asked Mr. Muston if he could present his findings to stimulate the Council's decision.

Mr. Muston thanked Chairman Nye and said he collected topic ideas as individual members relayed them.

Mr. Muston stated the first item addresses catastrophes. Reflecting on 9/11, a crisis existed in insuring commercial buildings. Mr. Muston presents these questions regarding this topic:

1. Can possible catastrophic events to critical infrastructure be conceived that might threaten the continuity and/or financial viability of critical infrastructure?
2. Is there insurance coverage for catastrophic events to ensure financial viability of critical infrastructure?
3. Are there Federal authorities for catastrophes, contingent on a catastrophe to trigger the authority?
4. Is it possible to use military forces and/or resources in the case of catastrophes affecting critical infrastructure?

Mr. Muston presented the second topic dealing with a regional cooperation framework. He made the following points:

- Events are likely to be local or regional and not likely to be nationwide;
- A Federal-level framework for cooperation has been set in motion;
- Various state and local programs have developed somewhat independently;
- What improvements in cooperative framework between local, state, and Federal authorities—including intelligence, law enforcement, first responders—and local critical infrastructure would be useful?
    - This entails preparedness, information sharing, and response

Mr. Muston noted the Council already addressed the third topic in its comprehensive Public-Private Intelligence Coordination Report and Recommendations. Nevertheless, critical infrastructure might benefit from additional updates to this report. Mr. Muston raised the following three points:

- Significant improvements have been made in the information sharing framework between the intelligence community, government, and critical infrastructure, but concerns remain about the appropriate forums, levels of disclosure, and authorities;
- The Federal government's own framework has undergone substantial change since the NIAC originally undertook its Intelligence Coordination study and regional centers have been established; and

- What additional steps might be taken to further improve this critical area of prevention and preparedness?

Mr. Muston presented the Council with a fourth topic dealing with CIP self-governance models. He posed the following questions to the Council:

- Can self-governance models be adapted to CIP needs of sectors?
- Do they offer values not met by present industry organization structures or regulatory frameworks?
- Can government benefit by understanding and encouraging these models as it considers its own role with critical infrastructure?

The last topic Mr. Muston addressed dealt with the international aspects of cyber crime. Some questions around this topic include:

- Are current policies and practices in the U.S. adequate to enable effective international cooperation in fighting cyber crime?
- Is the global framework for government and private-sector cooperation for investigation and enforcement adequate?
- Do U.S. law enforcement agencies need additional resources, tools, or organizations to manage cyber crime effectively?

By its very nature, cyber crime is global, presenting new challenges in the interpretation of law and enforcement.

Chairman Nye thanked Mr. Muston and pointed out none of the topics presented are incumbent from previous potential topics offered to the Council. He noted members made other suggestions outside of those presented by Mr. Muston, but some were left to the members themselves to monitor. Chairman Nye expected the White House or DHS would give the Council specific guidance. Absent that, Chairman Nye believed the NIAC should suggest what topics seem to have the most appeal to the Council. In that regard, the Chairman offered to keep a running list of ideas suggested by the Council. He suggested each member think of topics they believe optimize the Council's time and provide him with a brief description. He hoped the Council could pick one or more topics at its October fall meeting.

Chairman Nye asked if anyone wanted to comment. He added every member has been involved in one or more of the Council's projects. The NIAC's industrial expertise makes any topic fair game as long as the group keeps in mind not to make impractical commitments. With that, Chairman Nye opened the floor for discussion.

Assistant Secretary Stephan offered several observations. First, the White House, through Ambassador Thomas E. McNamara, Program Manager of Information Sharing Environment (ISE), recently designated DHS as the lead for the ISE architecture. The White House tasked OIP with integrating the private-sector component into a two-way information flow through all levels of government and the private sector. Assistant Secretary Stephan invited the Council to continue its studies in this area to aid OIP in its mission.

The Assistant Secretary commented on the fusion center phenomenon. There are now a large number of fusion centers across the U.S.—some tied to major municipal areas or multi-state regions. Figuring out how to insert the private-sector information-sharing piece into the architectures would be a timely topic.

Assistant Secretary Stephan noted regional organizations continue coordinating towards their own interests. Within the banking and finance world, the Pacific Northwest represents the first region to deal with security, restoration, and resiliency issues. Numerous examples such as this would be of interest to DHS to tap into this reservoir of thought and effort. DHS could use help in figuring out a plan to accomplish this.

Chairman Nye thanked the Assistant Secretary and added the NIAC remains ready to help DHS in any way. He asked if there were any comments from the members. He asked if Mr. Bossert, Ms. Sciarrone, and Ms. Kaufman wanted to add anything.

Ms. Kaufman pointed out that the Council might want to review the draft dates for the NIAC meetings over the next two years.

Chairman Nye pointed out meetings are all scheduled for the afternoon and asked the Council if an earlier time would be more convenient. He commented those dates need to be finalized soon. The Chairman added the Council might need to have a meeting in September in addition to their regularly scheduled meetings.

Chairman Nye asked the Council if any additional business needed to be addressed. The members voiced no concerns.

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

Chairman Nye thanked everyone for their support 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: 10/9/07_____
Erle A. Nye, Chairman

ATTACHMENT A

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

National Infrastructure Advisory Council (NIAC)

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

- Objective/Scope
- Key Questions
- Contributors
- Findings
- Recommendations

Objective

- Provide recommendations for preparing those who work in and maintain areas considered Critical Infrastructure (CI) for a chemical event and ensure they have the tools, training, and equipment necessary to identify, respond to and recover from a chemical 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 chemical preparedness and response programs?
- Question #3: Is there sufficient communication infrastructure in place to respond to a chemical event?
- Question #4: What tools and technologies currently support chemical 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

- Contributing government entities included:
  - DHS – multiple contributions
  - Georgia Army National Guard
  - National Library of Medicine (NLM)
- Contributing private sector entities included:
  - American Chemistry Council (ACC)
  - Chemical Sector Coordinating Council
  - BellSouth (AT&T)
- Critical sectors represented in the study group included:
  - Chemical
  - Communications
  - Emergency Services
  - Energy (Electric, Nuclear, Oil and Gas)
  - Financial Services
  - Food and Agriculture
  - Healthcare
  - Information Technology
  - Transportation
  - Water and Wastewater Management

Threats and Vulnerabilities

- Multiple T&V studies: DHS identified >3,400 chemical facilities where a release of chemicals threatens >1,000 people
- Chemical threats needs to be evaluated and bench-marked against comprehensive, national risk assessment priorities
- Chemical weapons or products synthesized for use as weapons
  - Chemical Weapons Convention (CWC) of 1993 named 29 specific substances and 14 broad families of chemicals that could be used as weapons: blister, blood, choking, nerve
  - Chemicals regulated by import/export controls and 1993 CWC
- Beyond military-grade substances, thousands of toxic industrial chemicals and agricultural pesticides could cause mass casualties

Surveillance and Detection

- Hazardous Substance Emergency Events Surveillance (HSEES)
  - CDC, Agency for Toxic Substances and Disease Registry, with 15 state health departments
  - Objective: Collect and analyze information about acute releases of hazardous substances that need to be cleaned up or neutralized according to federal, state, or local law, as well as threatened releases that result in a public health action such as an evacuation
- Toxic Exposure Surveillance System (TESS)
  - CDC with American Association of Poison Control Centers
  - Objective: Real-time national surveillance and exposure database
- National Incident Management System (NIMS)
  - DHS, FEMA
  - Objective: NIMS benefits include a unified approach to incident management; standard command and management structures; and emphasis on preparedness, mutual aid and resource management
- Electronic sensor capabilities:
  - Public sector: spectroscopic sensors, airborne spectral photometric collection technology, capillary electrophoresis
  - Private sector: electronic gas chromatography

Chemical Comprehensive Review

- Cooperative, government-led effort to enhance public safety by:
  - Integrating Federal, State, and local efforts
  - Preventing and preparing for potential terrorist attack
  - Identifying opportunities to reduce consequences of attack
  - Identifying opportunities to coordinate prevention and response capabilities
- Areas of focus:
  - Threat analysis
  - Facility characterization
  - Assault planning
  - Explosive ordinance disposal
  - Law enforcement resources
  - Emergency response resources
  - Maritime and transportation resources
- Better assess the risk of border controls/containment on chemical security.
  - Correlate border controls to other domestic chemical security measures; ensure consistency

From: DHS, Chemical Comprehensive Review, Regional Outreach Brief, May, 2007

Preparedness and Response

- Community Hazards Emergency Response-Capability Assurance Process (CHER-CAP)
- CHEMTREC drills and exercise program: HAZMAT response and containment
- Mutual aid organizations (e.g., chemical companies + public sector) and Fusion Centers
- Project Seahawk, Charleston, SC: integrated Federal, state, local, and private sector emergency response command center
- Community capability assessment tool (C-Cat)
- Emergency services capabilities assessment (ESCA)
- Buffer zone plan (BZP) technical assistance (TA)
- Chemical SSA-sponsored threat briefings and security teleconferences

Communications

- Pre-defined content
  - CDC emergency communications, staged short and long messages
  - Toxic Exposure Surveillance System (TESS) communication vehicle
  - CDC in collaboration with American Association of Poison Control Centers
  - Real-time national surveillance and exposure database; access to content
- DHS Report (8 Dec 06) on incident response communications interoperability
  - 22,400 randomly selected police, fire, and EMS agencies
  - Cross-jurisdiction interoperability outpacing federal to state or state to local interoperability progress
- SAFECOM
  - Established by the Office of Management and Budget
  - Provides research, development, testing and evaluation, guidance, tools, and templates on interoperable wireless emergency communications
  - Office of Emergency Communications
- WARN Act improvements to emergency communications

Chemical Facility Anti-Terrorism Standards

- Issued by DHS, effective June 8, 2007
- Objectives
  - Provide uniform national chemical facility security standards
  - Provide reasonable preemption if state laws conflict
  - Create protected Chemical-Terrorism Vulnerability Information (CVI) and ensure information dissemination to state, local, and other first responders
  - Ensure recognition of standards already achieved
- Process
  - More than 40,000 facilities must complete a consequence screening questionnaire
  - Risk rating by DHS
  - Vulnerability assessment for high risk facilities
  - Risk remediation plan; implementation
  - Audit and enforcement
- Project 5,000 – 8,000 high risk facilities; 300 in top two tiers

Sector Preparedness

- Well-prepared
  - Organizations with demonstrated capabilities on planning, preparedness, communications, and response tools/technologies
    - Large communications companies
    - Major metro Fire/EMS
    - Large IT companies
    - Chemical facilities
    - Nuclear facilities
    - Large healthcare, specifically tier-1 trauma centers
    - Large electricity companies
    - Finance, as part of broad all-hazards capability
    - Large water companies
- Chemical Sector
  - Self-organized American Chemistry Council (90% of industry production capacity) requires membership adherence to Responsible Care® program
  - ACC members invested $3.5B in security since 9/11
  - CHEMTREC® program 24/7 emergency response capability
  - TRANSCAER® nationwide transit incident responder assistance

Sector Preparedness (cont.)

- Moderately prepared
  - Organizations making progress on planning, preparedness, communications, and response tools/technologies
    - Transportation, specifically urban mass transit
- Limited preparedness
  - Organizations with limited or no capabilities on planning, preparedness, communications, and response tools/technologies
    - Broad food and agriculture
    - Small communications companies
    - Small fire/EMS
    - Small IT companies
    - Small electricity companies
    - Small water companies
    - Small metro transportation
    - Law enforcement

Recommendations

- Planning, preparedness, and response:
  - Complete the prioritization of comprehensive, national risk assessment that prioritizes chemical threats and vulnerabilities within context of others (e.g., CBRN.)
  - More clearly define roles and responsibilities for agencies that impact the transportation of, and accountability for, chemicals
  - Clearly define response roles, responsibilities, and communication protocols. Include as part of response exercises
  - Improve knowledge around specific scenarios, impact, and likelihood of events
    - Assess and/or improve usability/availability of planning data
    - Improve Chemical-Terrorism Vulnerability Information (CVI) availability
    - Fully deploy Chemical Security Assessment Tool
  - Improve planning, preparedness, and response capabilities across first responders
    - Improve accessibility and economic viability of necessary equipment
    - Improve readiness of first responders, especially law enforcement and Fire/EMS to address chemical events
    - Continue to staff and support Fusion Centers; better engage law enforcement in Fusion Centers

Recommendations (cont.)

- Surveillance and detection; tools and technologies:
  - Improve information collection, analysis, and reporting mechanisms that support chemical event detection; define S&T roadmap on same
  - Continue to fund collaborative, public-private efforts to develop more advanced detection solutions (Lawrence Livermore, Argonne, Brookhaven, Los Alamos)
  - Accelerate deployment of tools/technologies under development; identify commercialization or funding mechanisms making solutions more broadly available
- Communications:
  - Continue to make progress with NIMS/NRP 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.)

- Regulations:
  - Reduce duplicative regulations from multiple agencies; Develop and implement more efficient regulations that are risk- and threat-based and focused on achieving performance levels
  - Ensure all agencies follow DHS lead on facility and continue to support implementation of other agencies mission to address safety (OSHA), environment (EPA), and transportation (DOT)
  - Encourage public-private sector engagement; leverage existing coordinating council infrastructure
- International Policy:
  - Encourage full and global ratification and implementation of treaty requirements such as the Chemical Weapons Convention
  - Press for a level playing field on trade of chemicals; limit proliferation of chemicals as weapons
  - Drive global adoption of improved, risk-based site security measures
  - Address border control measures and ensure consistency of enforcement, including maritime
    - Correlate border controls to other domestic chemical security measures; ensure consistency
  - Provide incentives and support for global adoption of reasonable safety and security practices such as those being implemented by the International Coalition of Chemical Associations.

Questions?

ATTACHMENT B

The Insider Threat to Critical Infrastructures

ATTACHMENT B

The Insider Threat to Critical Infrastructures

National Infrastructure Advisory Council (NIAC)

The Insider Threat to Critical Infrastructures

Thomas Noonan
General Manager
IBM Internet Security Systems

Edmund Archuleta
General Manager
El Paso Water Utilities

Overview

- Objective
- Scope
- Phase I Preliminary Findings
  - Defining the Insider Threat to Critical Infrastructures
  - Analysis of the Dynamics and Scope
  - Defining the obstacles to addressing the insider threat
  - Analysis of the impact of Globalization on the Insider Threat
- Next steps
- Questions

Objective

- To define 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.

Scope

- Scope of the study (as outlined in the January 16 letter from Secretary Chertoff):
  - ✓ Define the "insider threat" physical and cyber, including potential consequences, economic or otherwise
  - ✓ Analyze the dynamics and scope of the insider threat including critical infrastructure vulnerabilities
  - ✓ Analyze the potential impact of globalization on the critical infrastructure marketplace and insider issues
  - ✓ Identify/define the obstacles to addressing the insider threat
  - ✦ Identify issues, potential problems, and consequences associated with screening employees
  - ✦ Identify legal, policy, and procedural barriers aspects of the issue, as well as any potential obstacles, from the perspective of the owners and operators
  - ✦ Identify and make policy recommendations on potential remedies for addressing the insider threat (up to and including potential legislation)

Preliminary Findings: Defining the Insider Threat to Critical Infrastructures

The January 16 letter to the NIAC stated**:** Define the "insider threat" for physical, cyber, and combined and include analysis economic consequences.

- *Definition:* the Insider Threat to critical infrastructure is 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
- Critical Infrastructure-level threats affect critical infrastructure services delivery, the national economic back-bone, or public health and safety

Preliminary Findings: Analysis of Dynamics and Scope of the Insider Threat

Scope:

- Focusing on Critical infrastructure level threats – those that affect CI services delivery, the economic back-bone, or public health/safety
- Variation among sectors on maturity and awareness
- Potential actors include: disgruntled employees, economic espionage, and infiltration

Dynamics:

- Lack of hard data for universal definition
- Globalization is escalating exposure and costs of these threats
- Technology and network risks rapidly escalating
- Complacency and denial are key components

Preliminary Findings: Defining the Obstacles to Addressing the Insider Threat

- Difficult to define due to lack of hard data
- Education and awareness is possible; needed cultural change is more difficult
  - Investment in structured programs and risk management
  - Corporate culture of trust runs counter to prevention programs
  - Workforce relations can complicate targeted efforts to address insider threats
- Use of background checks varies among sectors and are not universally accepted - regulation is controversial as a solution
- Multiple legal environments complicate Insider Threat mitigation strategies
  - Federal, state, local and multinational

Preliminary Findings: Analysis of the impact of Globalization

- Introducing enormous macroeconomic forces to the marketplace
  - Pushing large scale changes and introducing new threats for critical infrastructure operators
- Expanding IT networks and increasing risk
- Expanding the group of *insiders* - populations are less verifiable, and may be less reliable
- Varying legal environments among different countries
- Global supply chain used by infrastructure operators is increasing potential for expanded insider threats or *agents*

Next Steps

- Complete *Phase I* research
- Outline all secondary issues and their impact
- Draft recommendations
- Publish coordinating draft of report
- Begin *Phase II* research

Questions?

ATTACHMENT C

Future Work Topics

ATTACHMENT C

Future Work Topics

Future Work Topics

July 10, 2007

Agenda

- Framework for consideration of new topics
- Past accomplishments of NIAC
- Review known candidate topics
- Council discussion and input
- Schedule for new topic selection

Origins of Prior Studies

- Requests to the Council
  - Sector Partnership Model
  - Pandemic
  - Insider Threat
  - Hardening the Internet
  - Prioritizing Cyber Vulnerabilities
- Concerns put forward by NIAC Members

Accomplishments: Cyber Security

- Hardening the Internet
- Prioritizing Cyber Vulnerabilities
- Vulnerability Disclosure Framework
- Common Vulnerability Scoring Mechanism
- Convergence of Cyber Security & Protection of Physical Infrastructure

Accomplishments: Public – Private Cooperation

- Sector Partnership Model
- Public – Private Sector Intelligence Coordination
- Best Practices for Government Intervention
- Evaluation and Enhancement of Information Sharing and Analysis

Accomplishments: Roles of Government and Related Guidance

- Prioritization of Critical Infrastructure for a Pandemic Outbreak
- Cross Sector Interdependencies and Risk Assessment Guidance
- Risk Management Approaches to Protection
- Workforce Preparation, Education and Research

Ongoing Studies

- Chemical, Biological, & Radiological Threats
- Insider Threats

Potential New Topics

- The NIAC has considered potential new topics in the past
- The following ideas were gathered in these past exercises and from other inputs that have occurred since then

Dealing with Catastrophes

- Can possible catastrophic events to critical infrastructure be conceived that might threaten the continuity and/or financial viability of critical infrastructure?
- Insurance coverage for catastrophic events to ensure financial viability of critical infrastructure
- Federal authorities for catastrophes, contingent on a catastrophe to trigger the authority
- Use of military forces and/or resources in the case of catastrophes affecting critical infrastructure

Regional Cooperation Framework

- Events are likely to be local or regional
- A Federal-level framework for cooperation has been set in motion
- Various state and local programs have developed somewhat independently
- What improvements in cooperative framework between local, state, and federal authorities – including intelligence, law enforcement, first responders – and local critical infrastructure would be useful?
  - Preparedness, information sharing, and response

Intelligence Coordination & Information Sharing

- Significant improvements have been made in information sharing framework between the intelligence community, government, and critical infrastructure, but concerns remain about the appropriate forums, levels of disclosure, and authorities
- The federal government's own framework has undergone substantial change since NIAC originally undertook its study of intelligence coordination, and regional centers have been established
- What additional steps might be taken to further improve this critical area of prevention & preparedness?

Self-Governance Models for CIP

- Can self-governance models be adapted to critical infrastructure protection needs of sectors?
- Do they offer values not met by present industry organization structures or regulatory frameworks?
- Can government benefit by understanding and encouraging these models as it considers its own role with critical infrastructure?

International Aspects of Cyber Crime

- Are current policies and practices in the U.S. adequate to enable effective international cooperation in fighting cyber crime?
- Is the global framework for government and private sector cooperation for investigation and enforcement adequate?
- Do U.S. law enforcement agencies need additional resources, tools or organizations to manage cyber crime effectively?

Discussion

- What new topics merit consideration?
  - Past ideas
  - New ideas from Council Members