NATIONAL INFRASTRUCTURE ADVISORY COUNCIL (NIAC)

MEETING AGENDA

Tuesday, January 16, 2007
1:30 – 4:30 p.m. EST
National Press Club
529 14th Street NW
Washington, DC 20045

I.	**OPENING OF MEETING**	*Jenny Menna*, Designated Federal Officer, NIAC, Department of Homeland Security (DHS)
II.	**ROLL CALL OF MEMBERS**	*Jenny Menna*
III.	**OPENING REMARKS AND INTRODUCTIONS**	NIAC Chairman, *Erle A. Nye*, Chairman Emeritus, TXU Corp. *Michael Chertoff*, Secretary, DHS *George W. Foresman*, Under Secretary, Preparedness Directorate, DHS *Philip J. Perry*, General Counsel, DHS *Rear Admiral W. Craig Vanderwagen, MD*, Deputy Assistant Secretary for Preparedness and Response and Chief Preparedness Officer, Department of Health and Human Services *Neill Sciarrone*, Director of Protection and Information Sharing Policy, Homeland Security Council
IV.	**APPROVAL OF OCTOBER MINUTES**	NIAC Chairman, *Erle A. Nye*
V.	**FINAL REPORTS AND DELIBERATIONS**	NIAC Chairman, *Erle A. Nye* Presiding
	A. CONVERGENCE OF PHYSICAL AND CYBER TECHNOLOGIES AND RELATED SECURITY MANAGEMENT	*George Conrades*, Executive Chairman, Akamai Technologies, NIAC Member, *Margaret Grayson*, President, Grayson and Associates, NIAC Member, and *Gregory A.*

CHALLENGES	*Peters*, Managing Partner, Collective IQ, NIAC Member
B. DELIBERATION AND APPROVAL OF RECOMMENDATIONS OF FINAL REPORT	*NIAC Members*
C. PRIORITIZATION OF CRITICAL INFRASTRUCTURE FOR A PANDEMIC OUTBREAK IN THE UNITED STATES	*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 Rohde*, Chairman and CEO Emeritus, ConAgra Foods, Inc., NIAC Member
D. DELIBERATION AND APPROVAL OF RECOMMENDATIONS OF FINAL REPORT	*NIAC Members*
VI. NEW BUSINESS	NIAC Chairman, *Erle A. Nye*, NIAC Members
A. INTRODUCTION OF NEW WORKING GROUP TOPIC: ASSESSMENT OF THE INSIDER THREAT ON CRITICAL INFRASTRUCTURE	NIAC Members TBD
B. RECOMMENDATION FOLLOW-UP	*Sallie McDonald*, Director and Deputy Manager, National Communications System, Cyber Security and Telecommunications, DHS
VIII. ADJOURNMENT	NIAC Chairman, *Erle A. Nye*

MINUTES

NIAC MEMBERS PRESENT IN WASHINGTON:
Ms. Margaret Grayson and Mr. James Nicholson.

NIAC MEMBERS ATTENDING VIA CONFERENCE CALL:
Chairman Erle Nye, Dr. Craig Barrett, Mr. Alfred Berkeley, Chief Rebecca Denlinger, Lt. Gen. (ret.) Albert Edmonds, Chief (ret.) Gilbert Gallegos, Mr. Thomas Noonan, Governor Timothy Pawlenty, Mr. Bruce Rohde, and Dr. Linwood Rose.

MEMBERS ABSENT:
Mr. George Conrades, Commissioner Raymond Kelly, Ms. Martha Marsh, Mr. Gregory Peters, and Mr. John Thompson.

OTHER DIGNITARIES PRESENT:
Mr. Michael Chertoff, Secretary, Department of Homeland Security (DHS); Mr. George W. Foresman, Under Secretary, Preparedness Directorate, DHS; Mr. Philip J. Perry, General Counsel, DHS; Mr. Robert B. Stephan, Assistant Secretary, Office of Infrastructure Protection, DHS; Rear Admiral Craig Vanderwagen, Deputy Assistant Secretary for Preparedness and Response and Chief Preparedness Officer, Department of Health and Human Services (HHS); Neill Sciarrone, Director, Protection and Information Sharing Policy, Homeland Security Council; Sallie McDonald, Director and Deputy Manager, National Communications System, Cyber Security and Telecommunications, DHS; and Ms. Jenny Menna, Designated Federal Officer (DFO), NIAC, DHS.

I. OPENING OF MEETING

Ms. Jenny Menna introduced herself as the DFO for the NIAC. She welcomed Mr. Michael Chertoff, DHS Secretary; Mr. George W. Foresman, Under Secretary for Preparedness, Mr. Philip J. Perry, General Counsel, DHS; Mr. Robert B. Stephan, Assistant Secretary for Infrastructure Protection, DHS; Rear Admiral Craig Vanderwagen, Deputy Assistant Secretary for Preparedness and Response and Chief Preparedness Officer, HHS. Ms. Neill Sciarrone, Director, Protection and Information Sharing Policy, Homeland Security Council; Ms. Sallie McDonald, Director and Deputy Manager, National Communications System, Cyber Security and Telecommunications (CS&T); Mr. Erle A. Nye, NIAC Chairman; and all Council members present or on the teleconference. Ms. Menna also welcomed the members' staffs and other Federal government representatives. On behalf of DHS, she extended a welcome to members of the press and public. She reminded the members present and those joining via teleconference that the meeting was open to the public and, accordingly, they should remember to exercise care when discussing potentially sensitive information. Pursuant to her authority as DFO, Ms. Menna then called the 18th meeting of the NIAC and the first meeting of 2007 to order.

II. ROLL CALL

After calling the meeting to order, Ms. Menna then called roll.

III. OPENING REMARKS AND INTRODUCTIONS

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

Michael Chertoff, Secretary, DHS

George W. Foresman, Under Secretary, Preparedness Directorate, DHS

Philip J. Perry, General Counsel, DHS

Rear Admiral W. Craig Vanderwagen, M.D., Deputy Assistant Secretary for Preparedness and Response and Chief Preparedness Officer, Department of Health and Human Services

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

Chairman Nye thanked Ms. Menna for her introduction and informed the participants that the Council had enjoyed a tremendous year in 2006. The Chairman noted that the NIAC added three new members last year, adding that he hopes to add additional members in 2007. The Council, Mr. Nye explained, also produced two important reports in 2006:

- The Intelligence Coordination Report and Recommendations; and
- The Workforce Preparation, Education and Research Report and Recommendations.

The Convergence Working Group and the Pandemic Working Group also made significant progress on their reports during calendar year 2006, noting that each group will present their final reports to the Council at this meeting. In light of the conclusion of the Convergence and Pandemic Working Groups, Chairman Nye told the Council he anticipated that the White House and DHS would likely ask NIAC to pursue a new topic.

Chairman Nye asked DHS Secretary Michael Chertoff if he would like to add anything.

Secretary Chertoff thanked Chairman Nye and lauded him for his leadership on the Council. He also thanked all of the Council members for providing DHS and other Federal agencies with reports and recommendations, which will ultimately improve the protection and resilience of the Nation's infrastructure.

Noting that the NIAC's recommendations do affect DHS policy, the Secretary reminded meeting attendees about the importance of the Council's prior recommendation to form the Critical Infrastructure Partnership Advisory Council (CIPAC). On a related note, Secretary Chertoff announced the CIPAC is operational and has made significant strides. Citing the recent creation of the State, Local and Tribal Government Coordinating Council (SLTGCC), the Secretary said DHS continues to make real progress in solidifying the relationship between the public and private

sectors. DHS also continues to develop policy based on the Council's recommendations in its Intelligence Coordination Report and Recommendations and its Workforce Preparation, Education and Research Report and Recommendations. Furthermore, the Council offered important guidance in the development of the National Infrastructure Protection Plan (NIPP). Secretary Chertoff said DHS had received all 17 NIPP Sector-Specific Plans (SSPs) before the Department's deadline at the end of 2006. Currently, DHS is reviewing the SSPs, the Secretary said.

In his address to the Council, Secretary Chertoff said he anticipated hearing the final recommendations of the Pandemic Working Group. Acknowledging that he and Health and Human Services (HHS) Secretary Michael Leavitt had given the Working Group a very short timeline to complete its report, Secretary Chertoff said he believed the recommendations presented today will highlight the hard work and tremendous effort the Group put into this important endeavor. Thanking the Working Group in advance for their work, Secretary Chertoff said he planned to review the report immediately, adding that he had every confidence the report and recommendations would play a significant role in raising the Nation's level of pandemic preparedness.

The United States must prepare all Americans, including our Nation's critical infrastructure workers, well in advance of pandemic outbreak for the potentially severe medical and non-medical, economic, and social impact from such an event. The Secretary went on to say DHS remains proud of its efforts to prepare the private sector, particularly the critical infrastructure and key resources (CI/KR) community, for a severe pandemic influenza outbreak. DHS' *Pandemic Influenza Preparedness Response and Recovery Guide for Critical Infrastructure and Key Resources* (hereafter, the Guide), which the Department unveiled in September 2006, represents a major milestone in the Department's ongoing efforts to support pandemic planning in the private sector, Secretary Chertoff said.

The extreme scale and scope of a potential pandemic requires a dedicated effort and investment beyond typical business continuity planning. The Guide introduces a strategic framework that extends and refines business continuity planning based on an assessment of severe pandemic specific scenarios. Secretary Chertoff said DHS and its Federal partners remain committed to working with the Nation's CI/KR owners and operators to develop and implement effective business continuity plans ensuring continuous essential services remain functional and essential goods remain available during a pandemic.

Secretary Chertoff also expressed interest in hearing the final recommendations from the Convergence Working Group. The Secretary noted that the group's work and its findings are important because, as the technology for process controls systems (PCS) and supervisory control and data acquisition (SCADA) systems advances, government and industry must ensure the necessary safeguards are in place to minimize vulnerabilities and ward off threats.

With the completion of both Working Group reports, Secretary Chertoff asked, on behalf of the White House and DHS, the Council to turn its attention to a new matter, namely the insider threat to critical infrastructure. DHS and the White House would like the NIAC to provide recommendations clarifying the issues surrounding the conflict or potential conflict between privacy laws and counter-terrorism laws as they pertain to CI/KR employees.

Government and industry, the Secretary said, must be concerned about external threats to critical infrastructure, as well as the possibility of potential attackers within the infrastructure who may be a threat. Secretary Chertoff added that he looked forward to seeing the Council's progress on this topic at the next NIAC meeting in April.

Secretary Chertoff closed by informing the Council that DHS appreciates Council members' dedication and commitment to building and sustaining strong partnerships necessary to answering the critical infrastructure questions facing the United States.

Chairman Nye thanked Secretary Chertoff for his comments and asked Ms. Neill Sciarrone, Director of Protection and Information Sharing Policy at the Homeland Security Council, if she would like to address the Council.

Ms. Sciarrone thanked the Chairman and the Council members for the opportunity to speak with them, adding that the White House greatly appreciates all of the effort and time NIAC members put into their work. The Council's recommendations provide the White House with important insight.

Ms. Sciarrone also said the White House would like the NIAC to research and provide recommendations on the insider threat. At present, little research exists on the subject, and the Council's ultimate recommendations will create important policy on a relatively unknown subject, Ms. Sciarrone said.

Chairman Nye thanked Ms. Sciarrone and then introduced Mr. George Foresman, DHS Under Secretary for Preparedness.

The Under Secretary discussed his participation in a meeting of the National Security Telecommunications Advisory Council (NSTAC) earlier that morning. At the meeting, he said, NSTAC members discussed the significant challenges of the convergence of physical and cyber technologies, adding that the NSTAC planned to focus on this topic given its growing importance. Thus, with the NIAC Convergence Working Group's recommendations and the potential work of the NSTAC on the same subject, DHS will have plenty of background work from which to develop policy.

Chairman Nye thanked Under Secretary Foresman for his comments. He then introduced the meeting participants to Rear Admiral (RADM) Craig Vanderwagen, Deputy Assistant Secretary for Preparedness and Response and Chief Preparedness Officer, HHS. RADM Vanderwagen advises HHS Secretary Leavitt on matters relating to terrorism and other public emergencies.

RADM Vanderwagen thanked Chairman Nye and the Council, singling out the significance of the Council's work on a potential pandemic outbreak. He said pandemics are different from other national emergencies because they can occur across the country nearly simultaneously, a fact that created a significant need for cross-coordination between the public and private sector.

Given a pandemic's scope and scale, Americans should not expect the Federal government to handle all pandemic preparedness response and recovery efforts, the Rear Admiral said. To avoid economic

and social catastrophe, he added, pandemic preparedness demands full public and private sector engagement and participation.

RADM Vanderwagen praised the Council for its swift response to joint requests from Secretaries Chertoff and Leavitt, and in less than a year, they met the challenge. He stated it was an honor to accept the Council's Report and Recommendations on behalf of Secretary Leavitt, adding that he looked forward to working with the DHS and HHS partners to implement the Council's recommendations.

Chairman Nye thanked RADM Vanderwagen for his input and asked Mr. Robert Stephan, DHS Assistant Secretary for Infrastructure Protection, to make a few comments to the Council.

Assistant Secretary Stephan thanked Chairman Nye and told the participants DHS had realized a number of significant accomplishments in the Critical Infrastructure Protection arena in 2006. Over the past year, the Department saw extensive planning across all levels of government and between the public and private sectors.

Throughout 2006, DHS continued to develop new relationships and foster trusted partnerships across all levels of government and between the government and the private sector. Assistant Secretary Stephan noted that the work of the NIAC proved to be incredibly instrumental in the Department's ongoing efforts to bolster the public-private partnerships. Looking ahead to 2007, the Assistant Secretary said DHS and its partners would implement all the plans developed in 2006, including the 17 SSPs submitted in December by each of the 17 Sector Coordinating Councils (SCCs).

Assistant Secretary Stephan also told the Council he looked forward to working with the recommendations it made in the Convergence and Pandemic Reports and Recommendations.

The Assistant Secretary concluded by thanking the NIAC members for their hard work and leadership.

Chairman Nye thanked Assistant Secretary Stephan and asked DHS General Counsel Philip Perry if he had any comments he wanted to make.

Mr. Perry thanked Chairman Nye for the introduction and thanked the Council for the opportunity to participate in the meeting. It is the responsibility of the Office of General Counsel (OGC) to implement the Department's policy decisions. Over the course of the Department's brief history, policy implementation has proven difficult, Mr. Perry said, before noting that OGC had implemented more than 70 regulations and notices in 2006.

OGC not only drastically changed its regulations regarding the Critical Infrastructure Information Act (CIIA), it also revised the Safety Act regulations, Mr. Perry said. Per the NIAC's advice, OGC exercised its 871-exemption authority, which led to the development of CIPAC. Additionally, OGC promulgated a notice on chemical security regulations.

In his concluding remarks, Mr. Perry added that he anticipated rapid action across DHS' entire regulatory agenda. Before turning it back over to Chairman Nye, Mr. Perry echoed the sentiments of previous speakers by praising the Council for its work.

Chairman Nye thanked Mr. Perry for his comments.

Secretary Chertoff asked Chairman Nye if he could take a moment to recognize Assistant Secretary Stephan and Mr. Perry for their contributions to infrastructure protection. Assistant Secretary Stephan, Secretary Chertoff said, led the development of the NIPP and its 17 SSPs. The NIPP Base Plan and the SSPs represent a major accomplishment for DHS, Secretary Chertoff said, thanking the Assistant Secretary for his hard work. Secretary Chertoff also thanked Mr. Perry for his efforts to implement DHS regulations, which, he said, would help bolster national security.

IV.	**APPROVAL OF OCTOBER 10, 2006 MINUTES**	NIAC Chairman, *Erle A. Nye*, Presiding

Chairman Nye moved to the October meeting minutes. He asked the Council if there were any questions or comments about the minutes. Hearing no corrections or comments, he asked for a motion to approve the minutes. Mr. James Nicholson provided the motion which Mr. Gilbert Gallegos seconded. The Council unanimously approved the motion.

Chairman Nye introduced the Convergence Working Group's Final Report and Recommendations.

V.	**FINAL REPORTS AND DELIBERATIONS**	NIAC Chairman *Erle A. Nye* Presiding
	A. **THE CONVERGENCE OF PHYSICAL AND CYBER TECHNOLOGIES AND RELATED SECURITY MANAGEMENT CHALLENGES**	*George Conrades*, Executive, Fire Chairman, Akamai Technologies, *Margaret Grayson*, President, Grayson and Associates, NIAC Member; and *Gregory A. Peters*, Managing Partner, Collective IQ, NIAC Member

Chairman Nye introduced NIAC Member and Convergence Working Group co-chair Ms. Margaret Grayson, who, in turn, thanked the Chairman. Ms. Grayson began by saying the NIAC convened the Convergence Working Group in October 2005 to investigate the ongoing convergence of physical and cyber technologies for SCADA, PCS, and consolidated network management.
Control systems operate the physical infrastructures that distribute critical infrastructure services to the public and other infrastructure operators. The electrical grid and water distribution systems, which provide water and electricity to homes and businesses, serve as examples of vital SCADA systems in the United States. Other control systems operate processes to manufacture food or chemical products as well as to monitor and control natural gas pipelines and petroleum refineries. A cyber attack on these systems, Ms. Grayson explained, could potentially cause large-scale service interruptions, which may result in cascading effects into other economic sectors.

The Working Group assembled a Study Group made up of subject matter experts (SMEs) who informed the Group's work. Ms. Grayson conveyed her appreciation for the active participation and valuable contributions of these experts as the Working Group gathered information to complete its work.

The Working Group focused its efforts on identifying potential vulnerabilities in SCADA and PCS environments. The Group's policy recommendations would enable effective public-private partnerships to address cyber threats and improve the infrastructure protection profile of these critical systems.

The Group learned that, until recently, IT networks carrying business systems were not physically connected to control systems networks, and that the two systems failed to communicate, Ms. Grayson said. For a variety of reasons, increasing amounts of companies have created connections to their control systems in recent years; however, operators often remain unaware of the exposure these connections create. The growing connectivity of control systems creates new access avenues for potential cyber attackers. Strategic planning and coordination between public- and private-sector infrastructure protection partners is required to address the risk created by the convergence of control systems and IT systems in an adequate manner, Ms. Grayson noted. This NIAC study examined existing efforts to benchmark this problem and considered numerous available infrastructure protection models.

Over the course of their investigation, Working Group members gathered information from many sectors in this industry, spanning both government and private-sector operations. The study's preliminary findings highlighted the changing environment catalyzed by the convergence of control systems and IT systems, leading the Working Group to identify ways to strengthen current security practices through policy recommendations. The study only focused on SCADA and PCS environments prevalent throughout many of the critical infrastructure sectors. Other intersections of cyber and physical technologies, such as building automation, were deemed out of scope for this study.

To improve the public-private partnership and policy, Ms. Grayson said, the Working Group identified five key questions to study, including:

1. How can security be positioned as an enabler of the established goals of control systems operators?
2. What actions can be taken to improve market drivers for control systems security?
3. How can executive awareness be raised to facilitate a measured and appropriate response in the private sector?
4. What are the appropriate Federal government leadership roles and priorities for achieving control systems cyber security?
5. What policies and mechanisms would facilitate the needed information sharing to improve the cyber security posture of critical infrastructure control systems?

In the Convergence Working Group Report, each of the five key questions framed a series of findings and related recommendations. The Working Group's efforts involved providing actionable

and measurable recommendations to drive both immediate results as well as provide foundations for long term cooperation in a sustaining public/private partnership.

Each of the recommendations, Ms. Grayson said, includes a plan to identify the existing resources necessary to accelerate securing these critical systems.

The Working Group found business executives must fully understand the risk to control systems if they are to promote a corporate culture valuing cyber security as an enabler to control system operator goals of availability, reliability, and safety. To achieve this, Ms. Grayson said, critical infrastructure protection partners must educate executive leaders on the risk to their control systems and build the information sharing mechanisms necessary to understand the risk better.

Ms. Grayson outlined the Working Group's recommendations, which included:

1. The President consider establishing a goal for all critical infrastructure sectors that, no later than 2015, control systems for critical applications will be designed, installed, operated and maintained to survive an intentional cyber assault without critical function loss. This might seem aggressive, but information gathered by the Intelligence Community shows an increase in malicious intent that must be addressed.
2. DHS and SSAs collaborate with their respective owner/operator sector partners to develop sector-specific roadmaps using the Energy Sector Roadmap as a model. The Energy Sector adopted a self-regulatory approach providing a path and process that can act as a roadmap for other sectors that have not yet taken these steps.
3. DHS promote uniform cross-sector acceptance for prioritizing investment in control systems cyber security. For sectors with regulatory oversight of earnings and investments, DHS should promote including the costs of control systems cyber security as legitimate investments and expenses deserving of approval by their regulatory bodies. Cost remains a significant concern for adding security to existing SCADA infrastructures.
4. DHS and other relevant Federal agencies implement Convergence Study recommendations for improved information sharing.
5. DHS and other relevant Federal agencies implement Convergence Study recommendations for executive leadership awareness and the framework in Appendix A.

Each recommendation identifies DHS as the responsible party, since DHS' charter designates this role.

While researching the second question regarding market drivers, the Working Group found the early transition stage of the control systems market causes inconsistent market drivers across sectors to develop and implement secure products and systems. Security issues and needs awareness remains uneven across CI/KR sectors and prohibitive for most operators and vendors to develop and implement security features, Ms. Grayson reported.

The Working Group recommends:

1. The Office of Management and Budget (OMB) mandates Federal agencies apply the Cyber Security Procurement Language for Control Systems document and existing security and

security-relevant standards and criteria when procuring control systems and services. Leadership will come through Federal purchasing power.

2. Both DHS and the SSAs encourage applying existing security, security-relevant standards and criteria in developing and implementing secure control systems.
3. Both DHS and the SSAs encourage owners and operators to identify and utilize existing security, security-relevant standards and criteria for their control systems. The process of applying these standards and criteria will provide the basis for the continuing development of each operator's requirements to achieve control systems security.
4. SCCs apply the sector self-governance approach outlined in the framework of the NIAC's April 2004 Report and Recommendations on Best Practices for Government to Enhance Security of the National Critical Infrastructure with SSA validation for evaluation of self-governance effectiveness within each sector.

This requirement involves knowledge and awareness of existing security and security-relevant standards and immediate implementation of them as the first step in securing these systems. The Group asked that DHS step in as a diplomat, a leader, and an implementer.

While trying to answer the executive leadership awareness questions, the Working Group found executive awareness, within government and industry operators and vendors, of the cyber threat to control systems, remains critical to achieving all needed actions.

In response, Ms. Grayson said the Working Group recommended that DHS work with SSAs to implement a program for control systems cyber security executive awareness outreach. This outreach program, she said, would involve key elements, including:

- Value for senior executive-level decision-maker participants by including relevant strategic threat information gathered by the Intelligence Community;
- Establishing a continuing dialogue among parties relevant to critical infrastructure control systems in the public- and private-sectors, owner-operators, supporting government agencies and vendors involved in control system implementations, including IT and Security;
- A protected forum to discuss strategic information through CIPAC and the SCCs;
- Awareness outreach to address executive-level decision-makers in critical infrastructures, as well as owner-operators and relevant decision-makers in SSAs, State and local government;
- Strategic-level conversations to achieve operator vulnerability self-discovery, utilizing strategic-level information on threats, hostile actors, economic motivators for hostile actors and economic and physical consequences;
- DHS promotion of critical infrastructure control systems vulnerability assessments for development of corporate awareness; and
- Educating executives that control systems cyber security remain critical to the corporate operational safety goal.

The issue exceeds the importance of simple, risk assessment return on investment (ROI) decision-making. According to the report, the common decision-making corporate hierarchy goes in the following order of importance: 1) safety; 2) regulatory compliance; and 3) ROI. To achieve

appropriate investment for control systems security, Ms. Grayson said the discussion should be framed in terms of safety rather than ROI or risk assessment.

The questions focusing on government leadership priorities found strong, committed government efforts underway to address the cyber threat to control systems, Ms. Grayson said. To best address the cyber threat to control systems, government actions could benefit from private-sector feedback as well as higher-level interagency coordination and strategic planning.

In turn, Ms. Grayson outlined the Working Group's next series of recommendations. The Working Group recommends:

1. SSAs assign an Assistant Secretary-level senior executive leader responsible and accountable for their agency's collaboration with DHS efforts addressing their sector's control systems cyber security. This group should meet annually with the Partnership for Critical Infrastructure Security (PCIS) to evaluate each sector's strategy to meet the national control system survivability goal set for 2015, outlined in the "Security as an Enabler" section's suggestions for above.
2. The Federal government incorporates private-sector input into the cyber research and development (R&D) funding prioritization processes conducted by the Office of Science and Technology Policy (OSTP) and OMB. SSPs will provide initial input and SSAs will establish additional avenues for their sectors in the future.
3. DHS work with the Malcolm Baldridge Award for Excellence in Business Management and/or other similar programs to help communicate the importance of control systems cyber security to business leaders.

Regarding the question about information sharing, the Working Group found improved information sharing of control systems threats, vulnerabilities, consequences, and solutions remains vital to conduct a properly informed and measured response to the threat to critical infrastructure control systems.

The Working Group recommends:

1. DHS enhance the control system cyber incident information collection mechanism at Carnegie Mellon's Computer Emergency Response Team Coordination Center (CERT/CC) for collection, protection and sharing.
2. DHS rapidly ramp up CERT/CC's support services for control system operators to help develop a cyber incident information collection capability.
3. The Office of the Director of National Intelligence (DNI) develop a solution to the originator control (ORCON) problem currently preventing DHS from sharing threat information with critical infrastructure operators.
4. The Intelligence Community produce a Threat Assessment followed by a National Intelligence Estimate (NIE) for control systems threats to begin establishing a knowledge base.
5. DHS share relevant information from the Threat Assessment and NIE with critical infrastructure control systems operators.
6. DHS enhance existing program activities to create the ability to integrate and track understanding of the cyber risk for critical infrastructure control systems using all available sources.
   a. This collaborative program should collect, correlate, integrate and track information on:
      - Threats—including adversaries, toolsets, motivations, methods/mechanisms, incidents/actions and resources;
      - Consequences—including potential consequences of compromise to sector, industry, and facility-specific control systems; and
      - Vulnerabilities in control systems or their implementations in the IT infrastructure that adversaries could exploit to gain access to critical infrastructure control systems.
   b. This remains a DHS operations function and will include input and expertise from: critical infrastructure owner/operators and other relevant private-sector parties regarding consequences and vulnerabilities; the Intelligence Community on threats; CERT/CC and other sources on incidents; and DHS (including US-CERT) on cyber vulnerabilities.
   c. DHS will communicate the resulting warning information to control systems owner-operators to ensure protection of U.S. critical infrastructures.
7. The Program Manager, Information Sharing Environment, including information on control systems cyber threats in the Information Sharing Environment (ISE).

The achievement needed for the proper investment in cyber security for critical infrastructure control systems requires improved cyber incident information sharing for control systems. Currently, most control systems operators lack access to information regarding cyber incidents, because the needed mechanisms do not exist to adequately protect shared information. One reason for the lack of information is companies do not have a way to share this information safely and they fear losing the confidence of customers and investors if an incident became public, Ms. Grayson told the Council.

Chairman Nye thanked Ms. Grayson and the Working Group for their excellent work product. He asked the Council for a motion to approve the Convergence Report.

B. DELIBERATION AND APPROVAL OF FINAL RECOMMENDATIONS OF FINAL REPORT	*NIAC Members*

NIAC Member Mr. Alfred Berkeley motioned for the approval of the report and its recommendations. Dr. Craig Barrett seconded the motion, and they voted unanimously to send the recommendations to the White House.

C. PRIORITIZATION OF CRITICAL INFRASTRUCTURE FOR A PANDEMIC OUTBREAK IN THE UNITED STATES	*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 Rohde*, Chairman and CEO Emeritus, ConAgra Foods, Inc.

Chairman Nye then moved the conversation to the Prioritization of Critical Infrastructure for a Pandemic Outbreak in the United States Working Group's Final Report and Recommendations. The Chairman introduced Chief Rebecca Denlinger, the Co-Chair of the Working Group, to provide the recommendations.

Chief Denlinger thanked Chairman Nye and told attendees that the Working Group's final report addresses a significantly broader range of topics than her presentation discusses. Chief Denlinger said the Working Group focused its presentation on highlighting some key elements, the critical infrastructure worker specifically, of the final report.

As discussed at the October NIAC meeting, the very complex and deeply human nature of the prioritization question is far too critical to answer in purely mathematical terms, Chief Denlinger said. The Working Group assembled a prioritization framework identifying implementation principles and prioritizing the critical infrastructure workforce within this framework.

Chief Denlinger then asked Mr. Scott Blanchette, the substantive point of contact for Working Group Co-Chair Ms. Martha Marsh, to provide an overview of critical goods and services, the Working Group's prioritization schema, and critical workforce estimates.

Mr. Blanchette thanked Chief Denlinger and began his comments by explaining that the Study Group opened with a control set of assumptions and adopted the assumptions outlined in the National Strategy for Pandemic Influenza and the HHS Pandemic Influenza Plan. While the specific probabilities of some or all of these assumptions materializing remains up for debate, Mr. Blanchette acknowledged, the Study Group relied on these assumptions as an appropriate baseline from which to support the Working Group.

Mr. Blanchette said the Working Group identified three tenets of critical goods and services, including:

- Essential elements of national security and homeland security;
- Components of systems, assets, and industries upon which our economy depends; and
- Components of systems, assets and industries upon which public health depends.

The distribution of responsibility for much of the operations, maintenance, and sustainment of these critical goods and services resides within the private sector, Mr. Blanchette said. A consistent theme of the Pandemic Study Group's recommendations to the Working Group, he added, addressed the private sector's central role in any pandemic response scenario.

In addition to these key attributes, other factors elevate some key goods and services into a more critical status. Examples exist where some goods and services act as interdependencies to multiple other critical functions, Mr. Blanchette told attendees. For example, chemical production represents a critical interdependency for many sectors.

The impact of potential single points of failure represents another important finding in the Study Group's criticality assessment model. For example, the Food and Agriculture Sector possesses a high degree of production resiliency, capacity, and scalability allowing it to meet production and consumption benchmarks during a pandemic event, Mr. Blanchette said. However, critical single points of failure within the food and agriculture industry exist. For example, the Study Group found there are only six facilities that produce baby milk in the United States. The lack of redundancy in this production function, Mr. Blanchette said, suggests some critical risks in the Food and Agriculture Sector require additional consideration, study, and prioritization.

These priorities, interdependencies, and single points of failure generate a tremendous amount of discussion. To assist in producing its suggested recommendations to the Working Group, Mr. Blanchette said the Study Group used a mapping tool, which was populated with the results of the study that it commissioned to CI/KR sectors. The map reveals relationships between priorities, CI/KR sectors, and critical workers.

The gross volumes of workers identified as essential to operations within critical infrastructure represents the Pandemic study's first element. The study looked at 14 of the 17 CI/KR sectors, and included direct feedback from sectors to identify "essential workers" or relied on labor categories defined by the Bureau of Labor Statistics (BLS). The Study Group excluded some components of the Financial Services sector previously addressed in a more detailed and privileged study conducted by the Department of Treasury. Mr. Blanchette said additional refinement iterations might improve the quality of the data currently represented. For example, it is difficult to differentiate between an emergency services worker who might be a city-employed EMT and serve in the same capacity as a volunteer emergency services worker. The potential is high for this worker to be double-counted or excluded entirely, he said, noting data sources for those workers might opt to include or exclude this resource as part of the data collection effort. While there is significantly more work that could refine these numbers, it provides a general indication of essential workforce distribution across the 14 critical sectors included in this study, he said.

The study's second element is the gross volume of workers each sector identified as critical to sustaining operations in a pandemic. This number represents the figure identified by each sector as

the highest priority tier in a three-tier criticality scheme. For those sectors capable of differentiating between tiers, the Working Group further refined the prioritization of the workforce. For example, the communications sector identified roughly 800,000 members of its workforce as falling into one of the first three priority tiers. However, they only identified 400,000 workers as critical within the pandemic influenza context. These critical communications sector workers represented those responsible for communications management, operations, engineering, maintenance and administration. The highest priority workers within communications excluded those in many job categories, including sales, customer service support, legal, many elements of finance, human resources, facilities or other non-essential support functions.

Mr. Blanchette acknowledged that there is a great deal of work remaining to refine critical workforce estimates and reprioritize workforce at the most granular level possible. The Group identified the most critical workforce members during a pandemic event as those who deliver essential services. These workers include representatives who protect national and homeland security; ensure economic survival; and preserve public health and welfare.

Mr. Blanchette said the Group estimated 12.3 million Priority-1 critical infrastructure workers across all represented sectors. When benchmarked against other studies, this figure represents a departure in philosophy and implementation, as other similar studies had failed to account for critical infrastructure workers outside of the Public Health and Healthcare Sector.

For those who have or have not had the opportunity to study other sources of data, Mr. Blanchette said the NIAC study positions the critical infrastructure workforce more prominently than other approaches. For example, the Advisory Committee on Immunization Practices and the National Vaccine Advisory Committee included healthcare and EMS numbers similar to those represented in this study. However, those HHS-commissioned studies excluded many other critical infrastructure sectors, including Banking and Finance, Food and Agriculture, Postal and Shipping, and Transportation. As a point of reference, CI/KR priority workers represent only about 0.5 percent of the entire U.S. population, and this number becomes even smaller when solely focused on Tier-1 workers, Mr. Blanchette said.

Mr. Blanchette turned the floor over to Chief Denlinger to provide the Working Group's recommendations.

Chief Denlinger lauded both DHS and HHS for implementing a coordinated leadership team and supporting infrastructure in their combined efforts to continue to advance the Nation's pandemic influenza plans and programs.

Using a decidedly infrastructure-centric approach to this study, the Working Group suggests some opportunities exist to consider a differing prioritization framework and methodology, Chief Denlinger told the attendees. Specifically, Chief Denlinger suggested that the United States use the time before a pandemic as efficiently as possible. The Group recommends the NIAC ask the Federal government to pre-define, to the greatest extent possible, a consistent pandemic communications plan, complete with tailored communications to specific target audiences, which covers the entire pandemic episode. Additionally, the Pandemic Working Group recommends the Council ask the Federal government to develop and pre-position, again to the greatest extent possible,

communications in all distribution channels, including radio, television, telephone, print and online media. When working in concert and delivering a consistent message, these multiple distribution channels will provide the most optimal communications coverage to every target audience, the Chief said.

Chief Denlinger praised the work done to date with the private sector and critical infrastructure owner-operators on preparedness, adding that the Working Group recommended the Council ask the Federal government to continue engaging the private sector in augmenting the distribution of communications to the critical workforce. Finally, the Working Group suggested the NIAC ask the government to continue refining its communications plans, processes, and success metrics through a series of response exercises.

The tremendous progress made planning, rehearsing, and enabling communications, parallels the success stories in resource distribution and allocation across the country, the Chief said. For example, the Center for Disease Control (CDC) has performed some commendable work in prioritizing critical workers within the health and public health provider sub-sectors. These efforts should continue to garner the priority and attention they have warranted to date.

The Working Group recommended the continued development of a clearly defined vaccine and antiviral distribution strategy, and suggested that the government consider some of the prioritization elements identified in its presentation. More importantly, the Group suggested the government consider alternative distribution strategies and guidance to allow the private sector to distribute vaccines and antivirals to its in-scope critical workforce. It is unlikely government resources, at all levels, will be capable of reaching the entire critical infrastructure workforce in a timely, efficient and accurate manner. CI/KR owner-operators have tremendous transparency into the physical location and disposition of this workforce at nearly all times. This type of access and situational awareness could prove valuable as a component of a drug distribution strategy.

Chief Denlinger said the study suggested there is more work to accomplish to more clearly define response and containment roles and responsibilities. Confusion appears to exist over multiple Federal agencies' roles as well as how and when State, local, and private sector response participants will engage, in what capacity, and to what end. Similarly, the study also identified the need for more clarity around response timelines and milestones.

The Working Group believes there has been a good faith and generally successful effort made to educate stakeholders on existing plans. It recommends continued education efforts for all stakeholders on plans, process and priorities, Chief Denlinger said.

If the Federal government adopts the framework prioritization elements of this study, the Working Group would ask the Council to suggest developing a mechanism to identify priority workforce groups more clearly. For instance, who fits into a critical employee group will become a key tenet of any distribution strategy, and perhaps even more so when considering the distributed nature of the critical workforce member.

In response to the Secretaries' question about identifying principles for effective implementation, the Working Group opted to use the National Strategy for Pandemic Flu's three pillars as a framework.

Chief Denlinger said the Working Group believes the response plan and prioritization criteria, once agreed upon, remain fundamental to a successful response scenario. For the Nation to react in a coordinated, economical, and efficient manner, the Working Group asked the Council to recommend that subsequent communications, exercises, investments, and support activities align with existing plans and priorities. This alignment requires substantial executive level sponsorship, governance, and oversight to ensure permeation through all levels of government and industry. Simultaneously, this clear alignment of message and activity will eliminate ambiguity, reduce potential for error in response, and streamline response activities by focusing on what is deemed critical.

The remarkable surveillance and detection capabilities inherent in private industry today remain one of the study's remarkable yet intuitively obvious findings, Chief Denlinger said. While not specifically targeting pandemic flu, this private sector surveillance capability might potentially become a part of the National Response Plan (NRP). These resources appear throughout nearly every facet of the CI/KR and could augment traditional surveillance and detection infrastructures. The Group recommended extending surveillance to include occupational health professionals.

Additionally, the government should seek to engage the international components of U.S. corporations in global bio-data collection efforts, the Chief said. This partnership might further enhance data collection, aggregation, and analysis capabilities offered through relationships directly with host nations or other organizations, such as the World Health Organization (WHO).

The Working Group also recommended considering supplementing surveillance technology investments, acquisition, monitoring, and response capabilities to increase threat visibility and geographic coverage. Finally, it suggested the government engage non-traditional data acquisition and management resources within the commercial workforce in surveillance, collection, and analysis. Massive computing capabilities in the private sector not currently focused on this problem may significantly reduce the processing time required to identify a vaccine or anti-viral, or perhaps significantly increase the speed required to market either of these solutions.

As with any study where a group tries to arrive at a series of answers, the Working Group uncovered a number of questions along this path that members believe merit some further consideration, the Chief said. Multiple pieces of the data collection, analysis and prioritization challenges remain especially perplexing. The first is the reliance on foreign workers to support U.S critical infrastructure. For example, a tremendous amount of information technology support services come from offshore yet serve an absolutely critical function in the sustainment of many U.S. critical infrastructure operations.

Second, the Working Group identified a key weakness in the gross numbers of priority workers identified in their study: contracted workers. These resources provide essential services in nearly every sector, Chief Denlinger noted. The Nuclear Sector, for example, relies heavily on contracted resources for the support and maintenance of reactor facilities, yet sectors do not officially consider

these contracted workers part of the CI/KR. The Working Group recommended additional study on foreign workers supporting U.S. operations and the role and relevance of contracted resources currently unrepresented in their workforce model.

Chief Denlinger also suggested the workforce prioritization numbers presented in this study might be altered substantially with the implementation of specific government mitigation strategies during a pandemic. For example, government willingness to underwrite key components of the financial infrastructure might dramatically reduce the number of critical workers in many sectors necessary to sustain financial operations. The current vaccine and anti-viral production estimates may also put continued pressure on the need to refine the number of critical workers further. Regulatory relief, or relief from some regulatory mandates, may provide the potential to decrease the number of workers identified in Tier-1.

A number of competing strategies designed to prioritize scarce resources already exist. The Working Group reviewed strategies prioritizing specific metropolitan areas, at-risk populations, and critical goods and services. Chief Denlinger insisted that there must be continued dialogue on the specifics of these priorities and how trade-offs will continue to affect these interdependent populations.

A common theme throughout this study, the Chief said, is the impact of sick family members on the critical worker. There should be continued investigation of family member care, the containment impact on the critical worker, and the economical or efficient use of limited vaccine and anti-viral supplies.

Finally, the Working Group suggests some additional efforts should focus on studying the impact of potential containment strategies, such as closing U.S. borders or closing State borders, on organizations and their operations. Many organizations identified critical path issues associated with international and inter-state border and transportation management.

By placing a higher degree of priority on the critical infrastructure worker, Chief Denlinger said the Working Group offers a contrasting approach to previous studies, though the Chief was quick to point out that this study did not seek to understate the risk of other approaches, philosophies, or the populations addressed within those frameworks. It is the essential critical infrastructure worker, she said, who facilitates national and homeland security, ensures economic survival, and contributes to public health and welfare. Without these resources in a pandemic event, none of these strategic objectives are assured.

The Pandemic Group's final recommendation is three-fold:

1. The forum defined to continue this important study be fully implemented and supported. An extremely limited number of threats to the Nation exist that present the same potential for adverse impact on such a significant scale.
2. The Working Group suggests consideration be given to the distribution, response and communication approaches identified in this study. The CI/KR owner-operator is ready and committed to help the Nation prepare for and respond to a pandemic event.
3. After recognizing the many data collection, analysis, and prioritization challenges inherent in making human quality of life and livelihood determinations, the Working Group

recommends an appropriate forum or series of forums convene to refine the study of these numbers and continue to gain consensus on the approach and implications.

Chairman Nye thanked Chief Denlinger for her presentation and thanked the Working Group for its hard work. He then asked for a motion to accept the report and recommendations.

D. DELIBERATION AND APPROVAL OF FINAL RECOMMENDATIONS OF FINAL REPORT	NIAC Members

Mr. Edmund Archuleta motioned for the approval of the report and its recommendations. Mr. Gilbert Gallegos seconded the motion, and the Council voted unanimously to approve the Working Group's Final Report and Recommendations.

VII	**NEW BUSINESS**	NIAC Chairman, *Erle A. Nye*, NIAC Members
	A. INTRODUCTION OF A NEW WORKING GROUP TOPIC: ASSESSMENT OF THE INSIDER THREAT ON CRITICAL INFRASTRUCTURE	NIAC Members

Chairman Nye continued by introducing a new Working Group topic, Assessment of the Insider Threat on Critical Infrastructure. The Chairman then asked his substantive point of contact, Mr. William Muston, to provide the overview of the new topic.

Mr. Muston thanked the Chairman and told the meeting attendees his presentation would provide the elements of the request from the White House and DHS. The Federal government lacks an in-depth understanding of the concept of an insider threat to CI/KR, began Mr. Muston. The scope of the insider threat includes hostile acts, both physical and cyber, committed by employees of corporations and organizations in the position to exploit sensitive information. Thus far, no significant body of research on this topic exists, and the White House and DHS believe NIAC should formalize a study of this matter and provide policy recommendations on mitigating this threat and its impact on all CI/KR.

DHS and the White House requested multiple deliverables of the Council:

- Define the insider threat, both physical and cyber, and the consequences;
- Analyze the dynamics and scope of the insider threat;
- Define the obstacles to addressing the insider threat; analyze the potential impact of globalization of the critical infrastructure marketplace;
- Identify issues, potential problems, and consequences associated with screening employees;

- Identify the legal policy and procedural aspects of the issue, as well as any potential obstacles from the perspective of owners and operators; and
- Develop policy recommendations to mitigate the insider threat to critical infrastructures.

Chairman Nye thanked Mr. Muston and asked the members for any questions and comments regarding this request. He also asked the Council members if they believe they should accept this tasking from DHS and the White House.

Mr. Berkeley said the research for the new topic would potentially answer questions developed by owners and operators during the Intelligence Coordination Working Group's research. These private sector individuals wanted to understand the insider threat better and find a way to coordinate with the Federal government to help identify potential insider threats. Mr. Berkeley said he believed it would benefit the Council to take on this task.

Mr. Thomas Noonan told Chairman Nye the IT industry has questions regarding insider threats the Council could answer with this Working Group. Mr. Noonan then offered to co-chair the Working Group if the Council accepts the study request.

Providing background to the physical security side, Mr. Archuleta also offered to co-chair the Working Group.

Chairman Nye then asked for a motion for the NIAC to accept the insider threat task from the White House. Mr. Berkeley provided the motion. Mr. Gallegos seconded. The Council voted unanimously to accept the new topic.

Chairman Nye then turned the Council's attention to voting on the continuance of the Chemical, Biological and Radiological Events Working Group. The Council had previously halted the progress of the Working Group to turn its attention to the Pandemic Working Group, and specifically the requests from Secretaries Chertoff and Leavitt.

Chief Denlinger, the Working Group's previous co-chair, recommended the Working Group address the Chemical aspect of the Working Group first. She also offered to continue serving as the co-chair of the Working Group.

Chairman Nye then recommended that Mr. Bruce Rohde and Ms. Martha Marsh also participate in the Working Group; they previously co-chaired the Working Group with Chief Denlinger.

B. RECOMMENDATION FOLLOW-UP

Sallie McDonald, Director, National Communications System, Cyber Security and Telecommunications, DHS

Chairman Nye then introduced Ms. Sallie McDonald, the Director of the National Communications Systems (NCS) in the DHS Office of Cyber Security and Telecommunications (CS&T).

Ms. McDonald told the Council she wanted to address some of the issues the NIAC raised in its reports and listed some of the actions CS&T pursued in these areas. Ms. McDonald began with the Cross-Sector Independencies and Risk Assessment Guidelines Report and Recommendations that affected cyber and telecommunications, particularly those recommendations involving exercises. Cyber Storm, the recent national cyber exercise, enjoyed the critical infrastructure private-sector participation. With the Federal government scheduling the TOPOFF exercises and Cyber Storm exercises in alternating years, the Department will enjoy significant annual private-sector exercise participation.

In addition, the Internet Disruption Working Group (IDWG), co-sponsored by the National Cyber Security Division (NCSD) and NCS, held its first tabletop exercise with cross-sector Government representatives and private-sector Internet owners and operators in June 2006. IDWG plans to host annual meetings with cross-sector agencies and the private Internet community, including a tabletop exercise in the third quarter of fiscal year 2007.

The Common Vulnerability Scoring System (CVSS) Report features recommendations directed toward CS&T. One of the recommendations supported the use of CVSS by all Federal departments and agencies, Ms. McDonald said.

CS&T currently funds two projects addressing vulnerabilities and incorporating CVSS. Those two projects, explained Ms. McDonald, are The National Vulnerability Database (NVD), implemented and maintained by the National Institute of Standards and Technology (NIST), and the Common Vulnerability and Exposures (CVE) in the Open Vulnerability Assessment Language (OVAL) program. These programs are available for Federal entities, private-sector organizations, and the public, and they promote a common understanding of the severity of vulnerabilities.

Regarding the Prioritizing Cyber Vulnerabilities Report, CS&T asked lead agencies to work with each of the critical sectors to more closely examine the risks and the vulnerabilities of providing critical services over network-based systems. NCSD developed cross-sector cyber guidance with the Sector-Specific Agencies (SSAs) to consider cyber security as they develop their SSPs. A cyber security checklist was provided to these agencies to help ensure that cyber security is addressed throughout each plan in a consistent and appropriate manner.

The Hardening the Internet Report and Recommendations produced several recommendations affecting CS&T. Ms. McDonald discussed CS&T efforts in adopting security best practices. IDWG provided a final draft report last summer discussing best common practices for several Internet risk areas, including domain name servers and the border gateway protocol. IDWG also hosted a tabletop exercise in June 2006 where government and Internet industry representatives discussed best practices for Internet disruption risks. IDWG continues to work with private-sector experts to develop security fundamentals and guidance for tier two and tier three providers. This effort will complement other related activities in furthering the development of guidelines and best practices.

The Workforce Preparation, Education and Research Report and Recommendations contained numerous recommendations addressing CS&T. The recommendations in this report were assigned to all Federal agencies participating in the Cyber Corps or Scholarship for Service Program. The first recommendation involved revamping the Cyber Corps application process to mirror its

Department of Defense (DoD) counterparts. Representatives from the DoD Information Assurance Scholarship Program attend quarterly Cyber Corps Interagency Coordinating Council meetings co-chaired by both the National Science Foundation (NSF) and DHS. While the DoD program operates under different constraints in the Scholarship for Service Program than Cyber Corps, both groups are sharing best practices and placement tips.

The second recommendation sought to expand internship and employment options to include CI/KR owner-operators and government contractors performing specific document information assurance tasks for Federal, State, and local government. To broaden student placement opportunities across the Federal sectors, DHS and NSF supported agency briefings to educate hiring representatives and IT security program managers on the Scholarship for Service Program.

DHS and NSF also actively recruit agency participation in the annual Scholarship for Service job fair, Ms. McDonald noted. In January 2006, 320 students and 32 agencies attended the job fair, resulting in increased student placement rates. In addition, the Scholarship for Service Program is working in conjunction with the United States Secret Service (USSS) to provide interns annually to the 25 USSS electronic crime taskforces and working groups across the country. A draft Memorandum of Agreement is under review to launch the program in the fall of 2007. Through this partnership, Scholarship for Service interns will possess the opportunity to work with representatives from academia, the private sector, and various Federal, State, and local law enforcement entities.

The third recommendation addresses restructuring the scholarship funding. NSF leads a scholarship for service proposal review process annually and ensures subject matter experts thoroughly review the proposals. The Scholarship for Service grants are given out on the basis of merit and potential for positive impact in the cyber security education community. Students apply and receive their awards the Scholarship for Service scholarships via individual institutions.

The fourth recommendation wanted to lessen the challenge graduates face in obtaining a security clearance. The Scholarship for Service agreement requires students to be able to obtain a security clearance, placing the intern in positions with information of classified or sensitive nature. While DHS and NSF have no direct authority over the security clearance process, both organizations have taken proactive steps to educate students about what they need to do to prepare for the clearance process and how they can avoid common pitfalls. DHS and NSF invited an Office of Personnel Management (OPM) representative to the job fair to provide an overview of the clearance process, offering helpful guidance for proper completion of the paperwork, and explaining various types of clearances, as well as requirements, that may vary from agency to agency.

Another recommendation called for the development of a national agenda to prioritize cyber security research efforts. CS&T co-chairs with the Office of Science Technology Policy, the Cyber Security and Information Assurance Interagency Working Group. The Working Group serves as a part of the internal deliberative process of two sub-committees under the National Science and Technology Council. In May 2006, the Working Group published the Federal plan for Cyber Security and Information Assurance Research and Development. The Working Group will hold workshops with other government agencies, the private-sector, and academia to review the prioritized list.

The next recommendation suggested designating a privately administered public-private information assurance training certificate body. CS&T and other Federal agencies, such as DoD, cultivated relationships with the IT security certification vendor community. Through these relationships, agencies articulate the needs of the Federal workforce and incorporate them into certification products.

The final recommendation sought to review and reform information assurance procedures as required and provide outcome-based modular computer-based testing and metrics whenever possible. CS&T, Ms. McDonald said, will leverage the IT security professionals' common body of knowledge to work with IT security certification vendors to ensure certification tests accurately reflect the requisite knowledge skills and abilities.

Ms. McDonald closed by saying the implementations performed include some of the NIAC's recommendations CS&T implemented and plans to implement more in the future.

VIII. ADJOURNMENT

NIAC Chairman, *Erle A. Nye*

Chairman Nye thanked Ms. McDonald for providing the Council with an update of the implementation of their recommendations.

The Chairman concluded by saying the next meeting is scheduled for April 10, 2007 at the National Press Club in Washington, D.C. With this, Chairman Nye adjourned the meeting.

I hereby certify that 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: ___4/10/07___
Erle A. Nye, Chairman

ATTACHMENT A

The Convergence of Physical and Cyber Technologies and Related Security Management

National Infrastructure Advisory Council (NIAC)

Convergence Working Group

Final Report and Recommendations
January 16, 2007

George H. Conrades
Executive Chairman
Akamai Technologies

Greg Peters
Managing Partner
Collective IQ

Margaret Grayson
President, Grayson and Associates

NIAC WORKING DRAFT—NOT FOR REDISTRIBUTION

Overview

- Purpose
- Actions
- Timeline
- Potential NIAC Recommendations
- Next Steps

NIAC WORKING DRAFT—NOT FOR REDISTRIBUTION

Purpose

- Mission: The Convergence Working Group investigated important questions and to make recommendations regarding the protection of SCADA and Process Control Systems from cyber threats.

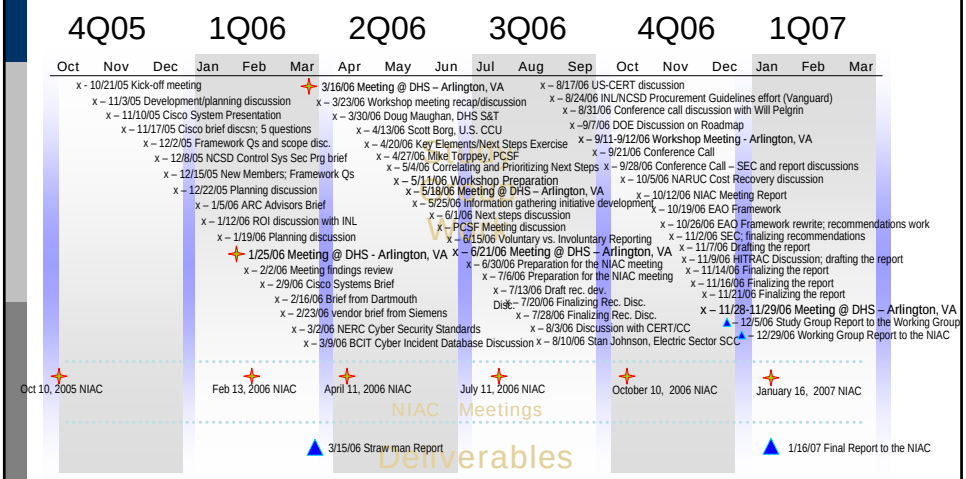
NIAC WORKING DRAFT—NOT FOR REDISTRIBUTION

Actions

- The Study Group doubled the pace of work in October and November - held 9 more (total of 52) conference call discussions to validate the recommendations and shape the Study Group Report.
- The Study Group held a 4-day workshop meeting at the end of November to rework the final Study Group Report to the Working Group.
- The Study Group Report was sent to the Working Group and selected subject matter experts on December 5, 2006.
- The Working Group Pre-briefed the White House regarding the potential recommendations on December 13, 2006.
- After feedback and revision, (including 4 more Working Group conference call meetings) the final Working Group Report was sent to the NIAC on December 29, 2006.

NIAC WORKING DRAFT—NOT FOR REDISTRIBUTION

Time Line



NIAC WORKING DRAFT—NOT FOR REDISTRIBUTION

Process: The Five Framework Questions

- ***Security as an Enabler*** **-** How do we position Cyber Security as a contributor and an enabler to achieving reliability, availability and safety goals in the management of SCADA and Process Control Systems?
- ***Market Drivers*** **-** What are the market drivers required to gain industry attention and commitment to research and product development?
- ***Executive Leadership Awareness*** **-** How do we best generate executive leadership awareness to assist in creating a culture and environment that values the protection of SCADA and Process Control Systems from cyber threats?
- ***Federal Government Leadership Priorities*** **-** What are the appropriate Federal Government leadership roles and priorities in identifying threats, vulnerabilities, risks and solutions?
- ***Improving Information Sharing*** **-** What are the obstacles and recommendations for improving information sharing about Process Control Systems and SCADA threats, vulnerabilities, risks and solutions?

NIAC WORKING DRAFT—NOT FOR REDISTRIBUTION

Recommendations for Security as an Enabler

The Working Group found that to promote a corporate culture where cyber security is valued as an enabler to control system operator goals of availability, reliability, and safety, executive leadership must fully understand the risk to control systems. To achieve this, critical infrastructure protection partners must educate executive leaders regarding the risk to their control systems and build the information sharing mechanisms needed to increase understanding of the risk.

Recommendations:

- The President establish a goal for all critical infrastructure sectors that no later than 2015, control systems for critical applications will be designed, installed, operated and maintained to survive an intentional cyber assault with no loss of critical function.
- The Department of Homeland Security (DHS) and Sector-Specific Agencies (SSAs) collaborate with their respective owner/operator sector partners to develop sector-specific roadmaps using the Energy Sector Roadmap as a model.
- DHS promote uniform acceptance across all sectors that investment in control systems cyber security is a priority. For sectors with regulatory oversight of earnings and investments, DHS should promote inclusion of the costs of control systems cyber security as legitimate investments and expenses that deserve approval by their regulatory bodies.
- DHS and other relevant Federal agencies implement Convergence Study recommendations for Improved Information Sharing.
- DHS and other relevant Federal agencies implement Convergence Study recommendations for Executive Leadership Awareness and the framework in Appendix A.

Recommendations for Improving Market Drivers

The Working Group found inconsistent market drivers across the sectors to develop and implement secure products and systems because the control systems market is in the early stages of a transition. Awareness of the security issues and needs is uneven across the critical infrastructure sectors, and the cost of developing and implementing security features is prohibitive for most operators and vendors.

Recommendations:

- The Office of Management and Budget (OMB) mandate that Federal agencies apply the *Cyber Security Procurement Language for Control Systems* document and existing security and security-relevant standards and criteria when procuring control systems and services.
- DHS and the SSAs encourage the application of existing security and security-relevant standards and criteria in developing and implementing secure control systems.
- DHS and the SSAs encourage owners and operators to identify and utilize existing security and security-relevant standards and criteria for their control systems. The process of applying these standards and criteria will provide the basis for continuing development of each operator's requirements to achieve control systems security.
- The Sector Coordinating Councils (SCCs) apply the sector self-governance approach outlined in the framework of the NIAC's *Best Practices for Government to Enhance Security of the National Critical Infrastructures*, April 2004, with validation by the SSA for evaluation of self-governance effectiveness within each sector.

Recommendations for Executive Leadership Awareness

The Working Group found that executive leadership awareness of the cyber threat to control systems, within government and industry operators and vendors, is critical to achieving all needed actions.

Recommendations:

DHS work with SSAs to implement a program for control systems cyber security executive awareness outreach. This outreach will include the elements outlined in the attached Framework in Appendix A. Key elements of the outreach program include:

- Value for senior executive-level decision maker participants through inclusion of relevant strategic threat information gathered by the Intelligence Community.
- Establishment of a continuing dialog among parties relevant to critical infrastructure control systems in the public- and private-sectors, owner-operators and supporting government agencies, and vendors involved in control system implementations, including IT and Security.
- A protected forum for discussion of strategic information through use of the Critical Infrastructure Partnership Advisory Council (CIPAC) framework and SCCs.
- Awareness outreach to address executive-level decision makers in critical infrastructures, as well as owner-operators and relevant decision makers in SSAs, State, and local government.
- Strategic-level conversations to achieve operator vulnerability self-discovery, making use of strategic-level information on threats, hostile actors, economic motivators for hostile actors, and economic and physical consequences.
- DHS promotion of critical infrastructure control systems vulnerability assessments for development of corporate awareness.
- The CIPAC structure was recommended by the NIAC as a result of the Sector Partnership Working Group Study and formally created by Homeland Security Secretary Chertoff in March, 2006.
- Education of executives that control systems cyber security is critical to the corporate goal of operational safety.

NIAC WORKING DRAFT—NOT FOR REDISTRIBUTION

Recommendations for Government Leadership Priorities

The Working Group found strong and committed government efforts underway to address the cyber threat to control systems. Government actions could benefit from private-sector feedback, and higher-level interagency coordination and strategic planning to best address the cyber threat to control systems.

Recommendations:

- SSAs assign a senior executive leader, at the Assistant Secretary level, as responsible and accountable for their agency's collaboration with DHS efforts to address control systems cyber security for their sector. This group should meet annually with the Partnership for Critical Infrastructure Security (PCIS) to evaluate each sector's strategy to meet the national control system survivability goal set for 2015.
- The Federal government incorporate private-sector input into the cyber research and development (R&D) funding prioritization processes conducted by the Office of Science and Technology Policy (OSTP) and Office of Management and Budget (OMB). Sector Specific Plans (SSPs) will provide initial input and SSAs will establish additional avenues for their sectors in the future.
- DHS work with the Malcolm Baldridge Award for Excellence in Business Management and/or other similar programs to help communicate the importance of control systems cyber security to business leaders.

NIAC WORKING DRAFT—NOT FOR REDISTRIBUTION

Recommendations for Improved Information Sharing

The Working Group found that improved sharing of information on control systems threats, vulnerabilities, consequences, and solutions is vital to a properly informed and measured response to the threat to critical infrastructure control systems.

Recommendations:

- DHS enhance the control system cyber incident information collection mechanism at Carnegie Mellon's CERT Coordination Center (CERT/CC) for collection, protection, and sharing.
- DHS rapidly ramp up CERT/CC's support services for control system operators to help develop a cyber incident information collection capability.
- The Office of the Director of National Intelligence (DNI) develop a solution to the problem of originator control (ORCON) that currently prevents DHS from sharing threat information with critical infrastructure operators.
- The Intelligence Community produce a Threat Assessment followed by a National Intelligence Estimate (NIE) for control systems threats to begin the process of establishing a knowledge base.
- DHS share relevant information from the Threat Assessment and NIE with critical infrastructure control systems operators.

NIAC WORKING DRAFT—NOT FOR REDISTRIBUTION

Recommendations for Improved Information Sharing *(continued)*

- DHS enhance existing program activities to create the ability to integrate and track understanding of the cyber risk for critical infrastructure control systems using all available sources.
- This collaborative program should collect, correlate, integrate, and track information on:
  - threats, including adversaries, toolsets, motivations, methods/mechanisms, incidents/actions, and resources;
  - consequences, including potential consequences of compromise to sector, industry, and facility-specific control systems; and
  - vulnerabilities in control systems or their implementations in the IT infrastructure that adversaries could exploit to gain access to critical infrastructure control systems.
- This capability is a DHS operations function, and will include input and expertise from: critical infrastructure owner/operators and other relevant parties in the private sector regarding consequences and vulnerabilities, the Intelligence Community on threats, CERT/CC and other sources on incidents, and DHS (including US-CERT) on cyber vulnerabilities.
- DHS will communicate resulting warning information to control systems owner-operators to ensure protection of U.S. critical infrastructures.
- The Program Manager, Information Sharing Environment, include information on control systems cyber threats in the Information Sharing Environment (ISE).

NIAC WORKING DRAFT—NOT FOR REDISTRIBUTION

Next Steps

- Full Council consideration/approval of the Final Report and Recommendations.
- Deliver NIAC Final Report and Recommendations to the President.

NIAC WORKING DRAFT—NOT FOR REDISTRIBUTION

Discussion

- Questions?

NIAC WORKING DRAFT—NOT FOR REDISTRIBUTION

ATTACHMENT B

Prioritization of Critical Infrastructure for a Pandemic Outbreak in the United States

National Infrastructure Advisory Council (NIAC)

NIAC Pandemic Working Group

Final Report and Recommendations
January 16, 2007

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.

NIAC WORKING DRAFT—NOT FOR REDISTRIBUTION

Requests from DHS & HHS Secretaries

Six Specific Pandemic Requests

1. Identify and define critical services to be maintained in a pandemic.
2. Establish criteria and principles for critical service prioritization.
3. Define critical services priority.
4. Identify critical employee groups in each priority critical service.
5. Build a structure for communication and dissemination of resources.
6. Identify principles for effective implementation by DHS and HHS.

NIAC WORKING DRAFT—NOT FOR REDISTRIBUTION

Assumptions

- Susceptibility to pandemic influenza virus will be universal.
- The clinical disease attack rate will be 30% in the overall population during the pandemic. Among working adults, an average of 20% will become ill from the pandemic influenza.
- Absenteeism may be as high as 40% during peak pandemic periods.
- Some will become sick from the pandemic influenza but not develop clinically significant symptoms. These persons can transmit pandemic influenza and develop immunity.
- Multiple waves of illness are expected with each wave expected to last 2-3 months.
- Each wave during its peak will adversely impact infected communities for 6-8 weeks.
- Effectively half of all infected will seek medical care.

Identifying Critical Goods and Services and Establishing Prioritization Criteria

Critical Goods and Services Identified

- Essential elements of ***national security and homeland security***
- Components of systems, assets, and industries upon which ***our economy depends***
- Components of systems, assets, and industries upon which ***public health depends***
- Fundamental to the 85% of the critical infrastructure owned and operated by the private sector
- Further defined by high rates of inter-dependency among critical infrastructure or single points of failure

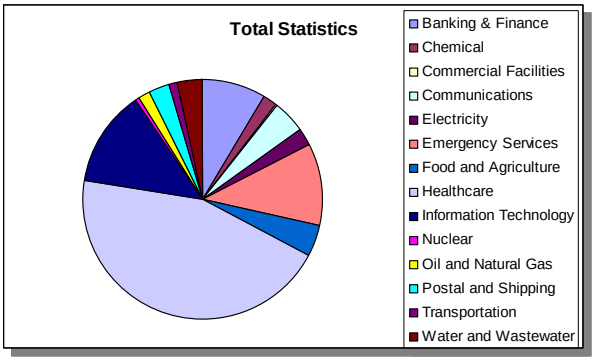
Criteria and Principles for Critical Service Prioritization Established

- **Critical goods/services required to *maintain national or homeland security***
  - For example: water, energy, food, banking & financial services, chemical, healthcare, Fire/EMS, communications, transportation, law enforcement, etc.
- **Critical goods/services to *ensure economic survival***
  - For example: banking & financial services, communications, IT, transportation, electricity
- **Critical goods/services to *maintain public health and welfare***
  - For example: water, energy, food and agriculture, healthcare, Fire/EMS, law enforcement, etc.
- **Critical goods/services with *significant number of inter-dependencies***
  - For example: water, electricity, food and agriculture, etc.

Identifying Critical Employee Groups Sector Detail: All Sectors, All Tiers

Critical Employees: Tiers 1 -3

Banking & Finance: 1,562,000
Chemical: 322,618
Commercial Facilities: 84,000
Communications: 796,194
Electricity: 375,000
Emergency Services: 1,997,583
Food and Agriculture: 750,000
Healthcare: 6,999,725
Information Technology: 2,359,800
Nuclear: 86,000
Oil and Natural Gas: 328,600
Postal and Shipping: 467,744
Transportation: 198,387
Water and Wastewater: 608,000



TOTAL: 16,935,651

Notes:

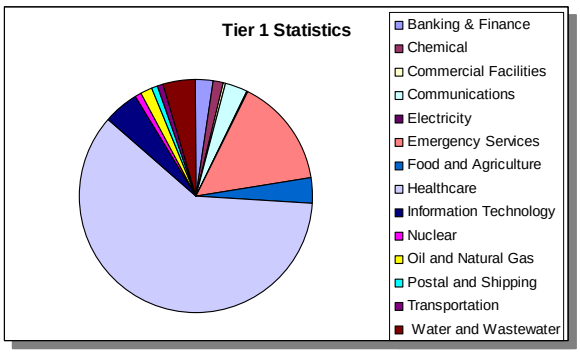
a. Numbers include Tier 1, Tier 2, and Tier 3 "essential" employees.

b. State and local government numbers removed from gross and priority workforce numbers.

Identifying Critical Employee Groups: All Sectors, Tier 1 Only

Employees: Tier 1 Only

Banking & Finance: 349,500
Chemical: 161,309
Commercial Facilities: 42,000
Communications: 396,097
Electricity: 50,000
Emergency Services: 1,997,583
Food and Agriculture: 500,000
Healthcare: 6,999,725
Information Technology: 692,800
Nuclear: 86,000
Oil and Natural Gas: 223,934
Postal and Shipping: 115,344
Transportation: 100,185
Water and Wastewater: 608,000



TOTAL: 12,322,477

Notes:

a. Numbers include Tier 1 "essential" employees only.

b. State and local government numbers removed from gross and priority workforce numbers.

NIAC Numbers: A Closer Look

- For good reason, the high percentage of Tier 1 Critical Workers identified from the Healthcare (HC) and Emergency Services (ES) sectors skews the overall data.
  - **NIAC's Tier 1 represents 14.5% of the entire 85 million U.S. CI workforce**, and only 4.8% for all sectors other than HC and ES.
  - When all tiers are included, the NIAC figure represents 19.9% of the CI workforce and 11.4% excluding the HC and ES sectors.
  - The total for all critical workers in all CI/KR sectors, including HC and ES, **equals only 0.5% of the total U.S. population**.
- In 2005, the Advisory Committee on Immunization Practices (ACIP) and the National Vaccine Advisory Committee (NVAC) provided prioritization recommendations, which HHS detailed in its Pandemic Plan.
  - NVAC/ACIP identified 17,034,000 CI/KR workers in Tier 1 (all in HC) and Tier 2.
  - The HHS Plan did not include several key CI/KR sectors, including **Banking & Finance, Chemical, Commercial Facilities, Food & Agriculture**, and **Postal & Shipping**.
  - Adjusting NIAC's figures to reflect only sectors included in the HHS studies reveals the **NIAC Tier 1 is 39.5% less than the total allotment of workers in the HHS plan**.

Recommendations

Building a Structure for Communication and Dissemination of Resources

Communications

- Pre-define, to the greatest extent possible, a consistent pandemic communications plan covering the entire pandemic episode; tailor public communications to specific target audiences.
- Develop and pre-position, to the greatest extent possible, public communications in all distribution channels, including radio, television, telephone, print, and online media.
- Engage the private sector to augment the distribution of public communications to the critical workforce; rehearse communication.
- Refine public communications plans, processes, and success metrics through series of response exercises.

Recommendations

Building a Structure for Communication and Dissemination of Resources

Dissemination

- Continue developing a clearly defined vaccine/anti-viral distribution strategy.
  - Consider alternative distribution strategies and guidance that allows the private sector to distribute vaccine and anti-viral medications to in-scope critical workforce.
- Clearly define response and containment roles and responsibilities.
  - Better define response timelines and milestones.
- Continue to educate all stakeholders on plans, process, and priorities.
- Develop mechanism to clearly identify priority workforce groups.
- Engage appropriate resources to ensure adherence to distribution strategy and the economical use of limited vaccine and anti-viral resources.
  - Identify, collect and report success metrics.

Recommendations

Identifying Principles for Effective Implementation by DHS and HHS

Pillar #1: Preparedness and Communication

- Clearly align preparedness and response plans, communications, exercises, investments, and support activities around sustaining critical workforce during pandemic influenza event.
  - Continue data gathering, analysis, reporting, and open review.
  - More clearly define roles and responsibilities across all stakeholders in both the public and private sectors.
  - Continue to develop and refine preparedness and response plans.
  - Continue to engage private sector in public sector planning and responses exercises.

Recommendations

Identifying Principles for Effective Implementation by DHS and HHS

Pillar #2: Surveillance and Detection

- Better engage key elements of the private sector in proactive surveillance and monitoring activities, including:
  - Extend surveillance to include occupational health professionals;
  - Engage international components of US corporations in global bio-data collection efforts;
  - Supplement surveillance technology investments, acquisition, monitoring and response, to increase threat visibility and geographic coverage; and
  - Engage non-traditional data acquisition and management resources within the commercial workforce in surveillance, collection, and analysis.

Recommendations

Identifying Principles for Effective Implementation by DHS and HHS

Pillar #3: Response and Containment

- Develop clearly-defined vaccine and anti-viral distribution strategy to ensure deployment as planned.
  - Consider alternative distribution methods that engage private sector directly distribute to in-scope critical workforce.
- Clearly define response and containment roles and responsibilities.
  - Better define response timelines and milestones.
- Educate all stakeholders on plans, process, and priorities.
- Develop mechanism to clearly identify priority workforce groups.
- Engage appropriate resources to ensure adherence to distribution strategy and the economical use of limited vaccine and anti-viral resources.
  - Identify, collect and report success metrics.

NOTE: Recommendations parallel Question #5, part-2, "Dissemination of Resources."

Additional Items, Possible Further Study

- Study impact of **foreign workers** on Critical Infrastructure (CI) operations.
- Explore the government's willingness to **underwrite key components of financial infrastructure** and provide **temporary regulatory relief**.
- Address **competing prioritization strategies** (e.g., key metro areas *vs.* CI, and at-risk populations *vs.* critical good/service producers).
- Study the impact of **contract resources and FTEs** on CI.
- Continue to investigate **family member care**, **containment impact** on the CI worker, and best use of **limited vaccine/anti-viral supplies**.
- Review **possible double-counted workers** (e.g., public/private/volunteer EMS; non-practicing MDs; and Federal/State/local and contract law enforcement).
- Study impact from **potential containment strategies** (e.g., border closures).

Final Thoughts

- **Existing Federal and State plan priorities include**:
  - Vaccine and anti-viral manufacturers
  - High-risk persons
  - Public health emergency workers
  - Key government leaders
  - Young and elderly individuals
- **NIAC prioritization focus differs from existing plans. Focus on**:
  - Maintaining national/homeland security, economic livelihood, and public health and welfare; and
  - Identifying and addressing critical inter-dependencies and single points of failure.
- **Suggest that resolution method be developed to determine**:
  - Federal/state prioritization method priority vs. NIAC recommended priority
  - Distribution methods: direct to private sector vs. direct to public sector
  - Further refinement of critical worker definitions, priorities, and numbers, including a possible forum to identify, quantify, and qualify ultimate prioritization and distribution methods.

ATTACHMENT C

New Initiative

Assessment of the Insider Threat to Critical Infrastructure

National Infrastructure Advisory Council (NIAC)

Possible New Initiative

Insider Threat to Critical Infrastructures

January 16, 2007

Overview

- Insider Threat
- Discussion
- Voting and Decision

Insider Threat

- Limited understanding and appreciation of the threats from insider attacks
- Scope includes hostile acts, both physical and cyber, committed by employees who use their privileges to exploit sensitive information
- Thus far, no significant body of research exists on the insider threat to critical infrastructure
- The White House and Department of Homeland Security believe the NIAC should formalize a study on this matter and provide policy recommendations on mitigating this threat and its impact on all critical infrastructures.

Requested Deliverables

- Define the "insider threat" both physical, cyber and consequence
- Analyze the dynamics and scope of the insider threat
- Define the obstacles to addressing the insider threat
- Analyze the potential impact of globalization of the critical infrastructure marketplace

Requested Deliverables (cont'd)

- Identify issues, potential problems, and consequences associated with screening employees
- Identify the legal, policy, and procedural aspects of the issue, as well as any potential obstacles, from the perspective of the owners and operators
- Develop policy recommendations to mitigate the insider threat to critical infrastructures

Voting and Decision

Discussion